مدخل في أمنية البيانات والمعلومات

ترجمة بتصرف لكتاب ويليام ستولنج

Cryptography and Network Security

Third Edition

by William Stallings

Lecture slides by Lawrie Brown

ترجمة وإعداد:

أ.فهد آل قاسم

مدرس مساعد جامعة العلوم والتكنولوجيا - فرع إب

Fahdalqasem.blogspot.com

fhdalqasem@yahoo.com

أمنية نظم المعلومات

الفصل	الصفحات
١	٤-٦-٧-٨-٩-١٠-١٢-١٣-١٤-١٥-١٦-١٧
٢	٤-٥-٦-٧-٨
٣	٤-٥-١٢-١٣-١٤-١٥-١٦-١٧-١٨-١٩-٢٠-٢١
٤	كل التعاريف
٦,٥	محذوف
٧	٨-٩-١٠-١١
٨	٣-٤-٥-٦-٧-٨-٨-٩
٩	٣-٤-٥-٦-٧-٨-٩-١٠-١١-١٢-١٣-١٤-١٥-١٦
١٠	٤-٥-٦-٧-٨-٩-١٠-١١-١٢-١٣-١٤-١٥-١٦-١٧-١٨
١١	٧-٨-٩-١٠-١١-١٢-١٣-١٤-١٥-١٦-١٧
١٢	MD5,SHA-1 full
١٣	٤-٥-٦-٧-٩-١٠-١١-١٢-١٣- dss- ١٧ - ١٨-١٩-٢٠
١٤	Kerbrose5
١٥	محذوف
١٦	
١٧	١٣-١٤-١٥-١٦-١٧-١٨-١٩-٢٠-٢١

الفصل الأول: مقدمة عامةintroduction

تعريفات هامة

أمنية الحاسوب computer security : إسم عام لمجموعة من الادوات المصممة لحماية البيانات وإعاقة القرصنة/ الهكر.

امنية الشبكات network security : مقياس او مقاييس حماية البيانات أثناء مرورها عبر الشبكة .

امنية الانترنت internet security : مقاييس لحماية البيانات اثناء مرورها عبر مجموعة من الشبكات المتصلة مع بعضها.

يهدف الكورس إلى دراسة امنية شبكات الانترنت.

- خدمة الامنية security service : هي الاشياء المحسنة لأنظمة معالجة البيانات، ونقلها عبر المنظمات.
  مقصودة لمقاومة الهجوم .
  يتم تقديم الخدمة عبر واحدة او مجموعة من آليات الحماية/ الميكانزمات.
  عادة يتم ربط الوظائف المكررة بوثائق مادية مثل :الحصول على توقيع مؤرخ، يحتاج إلى الحماية من الكشف ، العبث، أو التخريب، يجب ان يكون موثقا (بشهادة) مسجلة ومرخصة.
- آليات الأمنية security mechanism : الآلية المصممة للأعاقة والكشف والاصلاح من الهجمات المخلة بالأمنية.
  لا توجد ألية واحدة تدعم جميع الوظائف المطلوبة.
  ومع ذلك يوجد عنصر اساسي كآلية للحماية المستخدمةهو : تقنياتالتعمية (التشفير)، وهوما سوف يتم التركيز عليه.
- هجمات الأمنية security attack : أي حدث يهدد أمنية المعلومات المملوكة لمنظمة ما.
  تهدف امنية المعلومات إلى عرض كيفية منع هذه الهجمات او إفشالها.
- خدمات الامنية القياسية (x.800):

التحقق من الهوية Authentication: ضمان ان الجهة/الكائن المتصلة هي وحدها من تملك/تستحق هذه الميزة.

التحكم بالوصول access control : حماية الموارد من الاستخدام الغير مصرح به/ غير المخول.

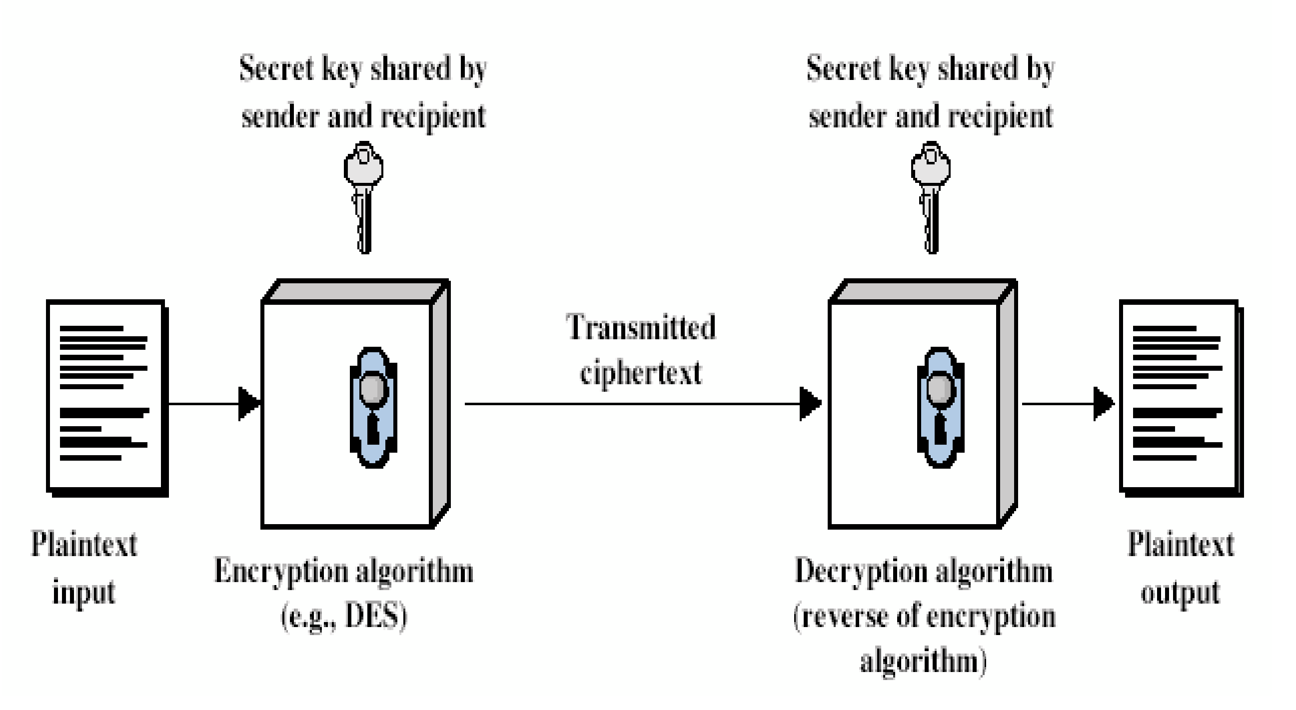
سرية البيانات data Confidentiality : هو حماية البيانات من الكشف الغير مصرح به.

سلامةالبيانات data integrity: هو ضمان ان البيانات المستلمة هي ذاتها البيانات المرسلةمن جهةمخولة بذلك/مصرح لها authorized.

عدم الانكار Non-repudiation: الحماية من إنكار الحدث من قبل أحد طرفي الاتصال المرسل/المستقبل مثلا.
- آليات معينة للحماية :
التشفير، التوقيع الالكتروني ، التحكم بالوصول، سلامة البيانات، تبادل الصلاحيات، المرور الزائد، التحكم بالمسار، الشهادة القانونية.
- آليات بينية للحماية (وسيطية):
الوظيفية الموثوقة، أغلفة الحماية، كشف الاحداث ، ممرات تدقيق الحماية، إصلاح الحماية (الخلل).
- تنصيف أنواع الهجمات التي تستهدف الامنية:
١.الهجوم السلبي passive attacks :
هو هجوم يتنصت على او يراقب حركة مرور البيانات بغرض :الحصول على محتوى الرسائل، أو مراقبة تدفق مرور البيانات.
٢.الهجوم الايجابي/ المؤثر active attacks :
عملية تعديل قناة البيانات من أجل :
التنكر كجهة موثوقة امام الاخرين، إعادة تشغيل/ارسال بعض الرسائل، تغيير مسار الرسالة، إنكار الخدمة.

الفصل الثاني: التقنيات القديمة للتشفير

- مصطلحات اساسية:
- **plaintext**: الرسالة الأصلية / المرسلة.
- - **ciphertext** الرسالة المشفرة .
- **cipher**: الخوارزمية المستخدمة لتحويل الرسالة الاصلية إلى رسالة مشفرة.
- **key**: معلومات مستخدمة للتشفير معروفة فقط للمرسل والمستقبل.
- **encipher (encrypt)**: عملية تحويل الرسالة الاصلية إلى الرسالة المشفرة (التشفير).
- **decipher (decrypt)**: عملية إستخراج والحصول على الرسالة الاصلية من المشفرة.
- **Cryptography**: علم دراسة التشفير الاساسيات/ الطرق.
- **cryptanalysis (codebreaking)**: تحليل الشفرة/ كسر الكود : علم يدرس عملية فك الشفرة في الرسالة المشفرة دون علم المفتاح.
- **cryptology**: المجال الذي يدرس علمي التشفير cryptography وتحليل الشفرة cryptanalysis.



Symmetric Cipher Model

- مطلبات التشفير التماثلي Symmetric Cipher الآمن هي :
- خوارزمية تشفير قوية.
- مفتاح سري معروف فقط للمرسل والمستقبل.
- علم التشفيروتحليل التشفير Cryptography:

يمكن ان يوصف بـعدة عوامل هي :
١. نوع عمليات التشفير المستخدمة.
٢. عدد المفاتيح المستخدمة (واحد خاص، إثنين عام).
٣. طريقة معالجة الرسالة الاصلية : الوحدة/القالب أو القناة.

- أنواع هجمات تحليل الشفرة Cryptanalytic Attacks التي تعني كسر الكود بدون معرفة المفتاح :

- **ciphertext only** :
  - يعرفون فقط الرسالة المشفرة والخورازمية وببعض الاحصاءات يحصلون على الرسالة الاصلية.
- **known plaintext**
  - يعرفون الرسالة الاصلية والمشفرة ويهدفون إلى فك خوارزمية التشفير.
- **chosen plaintext**
  - إختيار رسالة اصلية من مجموعة خيارات للحصول على الرسالة المشفرة بهدف فك الخوارزمية.
- **chosen ciphertext**
  - إختيار رسالة مشفرة من مجموعة خيارات للحصول على الرسالة الاصلية بهدف فك الخوارزمية.
- **chosen text**
  - يوجد خيارات الحصول على الرسالتين الاصلية والمشفرة بهدف فك الخوارزمية ومعرفة طرق التشفير وفك التشفير.

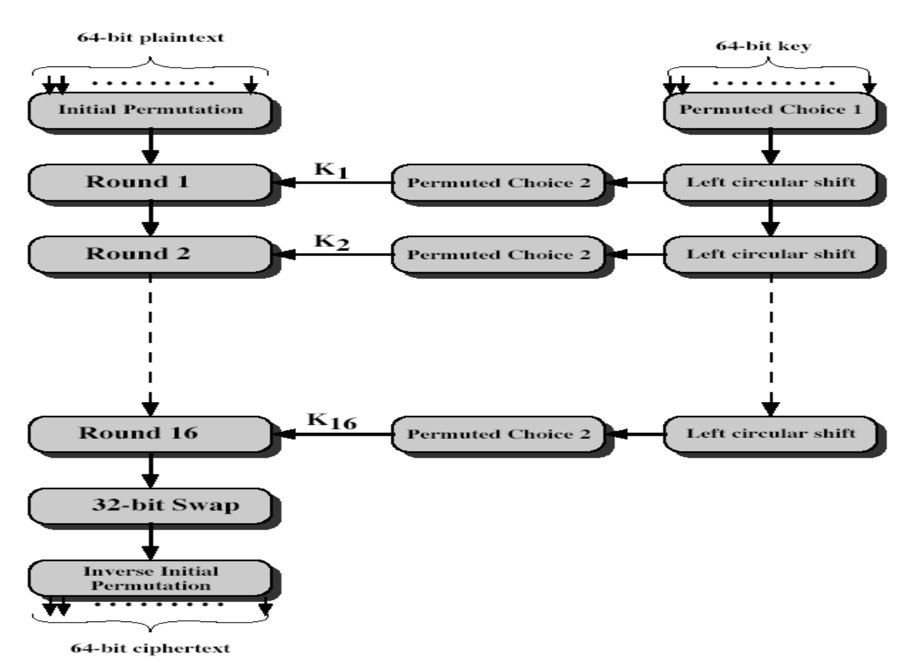
الفصل الثالث: التشفير القياسي للبيانات
Block Ciphers and the Data Encryption Standard

مقارنة التشفير بالقناة/قناة البتات (stream) والتشفير بالقالب/وحدة البتات(block):
* يتم معالجة الرسائل في حالة التشفير بالقالب كمجموعة من البتات يتم تشفيرها معا، طول القالب ٦٤ بتا او اكثر.
* يتم معالجة الرسائل في حالة التشفير بالقناة في الوقت الواحد بتا أو بايتا واحدا، يتم تشفيره.
* أغلب ادوات التشفير حاليا هي من النوع التشفير بالقالب.

- الطريقة القياسية لتشفير البيانات Data Encryption Standard (DES):

من اكثر الوسائل المستخدمة في العالم، قدمت عام ١٩٧٧بواسطة معهد NBS الذي اصبح اسمه الآن NIST.
يشفر قالبا مكون من ٦٤ بتا بواسطة مفتاح طوله ٥٦ بتا، هناك جدل بشأن جدوى امنيته.
لمحة تاريخية ....

- DES Encryption:



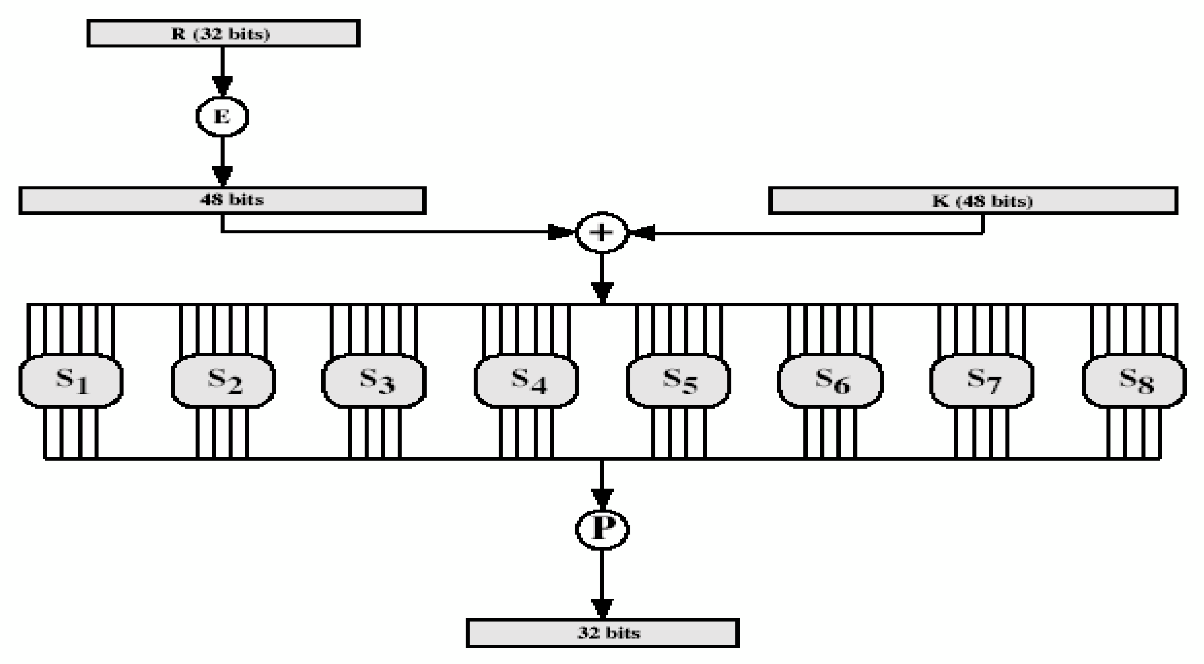
الخطوة الاولى هي عملية إطلاق التباديل Initial Permutation، التباديل الابتدائي وفيها يتم عمل تباديل رياضية على البتات الداخلة.

في المرحلة التالية: مرحلة الدورات الهيكلية DES Round Structure، حيث تمر العملية بست عشرة دورة في كل دورة يتم اضافة مفتاح التشفير بطريقة معينة.
وفي كل دورة يتم عمل الخطوات التالية:
يجزء القالب إلى نصفين كل نصف ٣٢ بت، يتم تحديد قيمة كل بت في كل نصف كما بالعلاقة :

$L_i = R_{i-1}$

$R_i = L_{i-1} \text{ xor } F(R_{i-1}, K_i)$

وكما بالشكل ادناه يتم اخذ النصف الايمن وتطبيق الدالة E التي تحوله إلى ٤٨ بت، وتضيف هذه البتات إلى عدد مشابه يمثل جزء من المفتاح المستخدم في التشفير.
تمر النتيجة التي نحصل عليها بثمانية صناديق يقوم كل صندوق بإستقبال ستة بتات من الـ ٤٨ بتا، ويحولها بطريقة معينة إلى اربعة بتات، مما يحول الناتج النهائي إلى ٣٢ بتا، نقوم قبل ذلك بعمل تباديل رياضية عليها.



الصناديق الثمانية Substitution Boxes :
كل صندوق كما اسلفنا يحول الـ ٦ بت إلى اربعة بتات، يأخذ الصندوق البت الاول والاخير (واحد وستة) ليعمل منها صف، ويعمل من الاربعة بتات الداخلية اربعة اعمدة، ليطبق عمليات رياضية معينة، يجب ان تضمن هذه العملية سلامة الانعكاس بالنسبة للطرف الآخر الذي يفك التشفير، ويقوم هذه الجدول المكون من اربعة اعمدة وصفين بإنتاج اربعة بتات مقابلة، هي التي يقوم كل صندوق بإخراجها.
وهي عملية في مخرجاتها تشبه ما يفعله الضغاط من ضغط المدخلات وتحويلها إلى حجم اقل.
مثال بالنظام الست عشري: S(18 09 12 3d 11 17 38 39) = 5fd25e03
جدولة المفاتيح الفرعية DES sub keys generating:
يتحول مفتاح التشفير كما هو موضح بالشكل، إلى ستة عشر مفتاح فرعي، يدخل كل واحد منها إلى كل دورة من الدورات التي تمر بها قالب الرسالة نفسه.
يتم في البداية بمجرد إدخال مفتاح التشفير تطبيق عمليات تباديل رياضية أولى (pc1) أو permutation choice1 والتي تقوم بإختيار ٥٦ بت من الـ ٦٤ بت المكونة للمفتاح، ومن ثم تقسم هذه الـ٥٦ بت إلى نصفين كل نصف ٢٨ بتا.
يمر المفتاح بعدها بست عشرة مرحلة تطبق عليه في كل مرحلة العمليات التالية:
ـ يتم اختصار كل نصف من ٢٨ بت إلى ٢٤ بت .
ـ عملية التباديل الرياضي الثانية pc2 تطبق في كل مرحلة.
ـ يطبق على المفتاح الفرعي عملية تدوير مكررة لكل نصف مكان الآخر، سواء مرة او مرتين، حسب رقم المرحلة k.

- العمليات الخاصة بفك الشفرة DES Decryption :

تقوم خوارزمية فك الشفرة بعمليات عكسية لكل خطوة من تلك الخاصة بخوارزمية التشفير، تولد المفاتيح الفرعية بطريقة عكسية ايظا، وتطبق بترتيب عكسي، وكذلك بالنسبة لعمليات التباديل وغيرها من العمليات.

الفصل الرابع: الحقول المنتهية
Finite Fields

التعاريف الرئيسة

- الزمرة group : هي مجموعة من العناصر او الارقام، مع مجموعة من العمليات الجبرية (عملية واحدة في الغالب) التي نواتجها ضمن هذه المجموعة (عمليات مغلقة)، وتحقق الشروط التالية:

قانون التجميع للعملية: associative law $(a.b).c = a.(b.c)$

وجود عنصر محايد للعملية: has identity e $e.a = a.e = a$

وجود النظير المقابل: has inverses a-1 $a.a\text{-}1 = e$

وإذا كانت العملية تبادلية $a.b = b.a$، سميت الزمرة بالزمرة التبادلية abelian group.

- وتسمى الزمرة بالزمرة الدورية cyclic group، إذا استطعنا توليد جميع عناصر الزمرة برفع عنصر ثابت منها إلى اسس مرتبة، يسمى العنصر الثابت بمولد الزمرة حيث :

a هو مولد الزمرة هنا، إذا كان $b = a^k$ حيث b يمثل جميع عناصر الزمرة، من اجل قيم مختلفة لـ k.

الحلقة Ring : هي مجموعة من الاعداد التي تطبق عليها عمليتين (ضرب وجمع) وتحقق:

- زمرة تبديلية abelian group على عملية الجمع.
- عملية الضرب تجميعية associative، مغلقة، توزيعية distributive بالنسبة لعملية الجمع أي أن:

$$a . (b + c) = a . b + a . c$$

- وإذا كانت عملية الضرب تبديلية، سميت الحلقة بالحلقة التبديلية commutative ring.
- وإذا كانت عملية الضرب تملك نظائر (دون قاسم صفري)، فإنه تشكل فضائي تكامليا/ متمما integral domain.

- الحقل Field: هو مجموعة مكونة من عناصر او ارقام مع عمليتين يحقق:

- زمرة تبديلية بالنسبة للعملية الاولى (الجمع).
- زمرة تبديلية بالنسبة للعملية الثانية (الضرب)، بإستثناء الصفر.
- يحقق شروط الحلقة للمجموعة مع العمليتين.

- الموديول الحسابي Modular Arithmetic :

يعتني بتعريف مؤثر الموديل mod الذي يحقق :

a mod n هو باقي قسمة a على العدد n.

نستخدم التعبير a=b mod n إذا كان باقي قسمة أي من العددين a,b على n هو نفسه، مثلا: 5=17 mod 12 .

العبارة a=b mod n يمكن ان تكتب رياضيا $a = qn + b$، حيث ان $0 <= b <= n-1$

يمكن عمل جدول خاص بكل عدد صحيح يسمى modulo n، يحتوي على جميع العناصر المتقابلة عند تطبيق المؤثر mod، عليها.

مثال جدول يوضح موديلو للعدد ٧ (Modulo 7 Example):

...						
-21	-20	-19	-18	-17	-16	-15
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	**1**	**2**	**3**	**4**	**5**	**6**
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	32	33	34
...						

- القاسم divisors

نقول ان العدد الصحيح غير الصفري b انه قاسم لـ a إذا كان يوجد عدد صحيح m بحيث أن : a = m . b ، وهذا يعني ان a يقبل القسمة على b بدون باقي.ويرمز لهما بـ b!a.مثلا الاعداد ١,٢,٣,٤,٦,٨,١٢,٢٤ كلها تقسم العدد ٢٤.

- عمليات الموديول الحسابي Modular Arithmetic Operations:

يستخدم الموديل الحسابي الاعداد المنتهية القيم، وذلك لجعل عملياتها تعطي نتائج حلقية/دورانية تنتهي لتبدأ من أول قيمة.

يمكن تعريف الموديل الحسابي لأي زمرة من الاعداد الصحيحية مثلا:

$$Zn = \{0, 1, \dots , n-1\}$$

وهذه الزمرة تشكل مع عمليتي الجمع والظرب حلقة تبديلية. الشكل التالي يوضح $(Z_8 , +)$:

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

(a) Addition modulo 8

- القاسم المشترك الاعظم Greatest Common Divisor (GCD) :

مسألة مشهورة في نظرية الاعداد، القاسم المشترك الاعظم GCD للعددين b , a هو اكبر عدد صحيح يقبل العددان القسمة عليه (يقسمهما)، مثلا GCD(60,24) هو العدد ١٢.

- خوارزمية إقليدس للقاسم المشترك الاعظم Euclid's GCD Algorithm :

هي طريقة مشهورة لتسهيل عملية للحصول على الـ GCD، وتنص على أن :

القاسم المشترك الاعظم لعددين يساوي القاسم المشترك لأحدهما مع باقي قسمة الآخر عليه.

GCD (a , b) = GCD (b , a mod b)

ميزة هذه الخوارزمية هي تسهيل عملية الحصول على الـ GCD، في العمليات الكبيرة مثلا الـ GCD(٧,٨٠) تؤول إلى GCD(٧,٣) وذلك لأن 80 mod7= 3، وحساب عوامل الـ ٣ اسهل بالتأكيد من حساب عوامل الـ ٨٠. وهكذا..

ويمكن تنفيذ هذه الخوارزمية حاسوبيا كالتالي:

- A=a, B=b
- while B>0
  - R = A mod B
  - A = B, B = R
- return A

- حقول جلويس Galois Fields :

هي حقول منتهية، تلعب دورا هاما في نظريات وطرق التشفير.

بتطبيقها يمكننا الحصول على عدد من العناصر في حقول منتهية finite fields بشرط ان اساس لعدد اولي من الشكل P^n ، يرمز بالرمز $GF(P^n)$، وفي العادة يتم استخدام الحقول المولدة من الشكلين:

- GF(p)
- GF(2n)

حيث ان GF(p) مجموعة الاعداد الصحيحة من ١ إلى p-1، مع الموديول الحسابي موديلو p.

وهذا الشكل يحقق شروط الحقول المنتهية، وتتميز هذه الحقول بتطبيق عمليات الجمع والظرب (وبالتالي القسمة والطرح) دون الخروج عن حدد المجموعة.

المثال الموضح في الجدول ادناه يوضح نواتج الحقل (* ,FG(7)):

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$ ι modulo 7

وبخصوص كثيرات الحدود فإننا نهتم بموديلو ٢ حيث تكون المعاملات اما ٠ أو ١ .
فعند جمع كثيري حدود يتم إعتبار المعاملين ١,٠ فيكون ناتج جمع وضرب كثيري الحدود، كما في المثال:

– eg. let $f(x) = x3 + x2$ and $g(x) = x2 + x + 1$
  $f(x) + g(x) = x3 + x + 1$
  $f(x)$ x $g(x) = x5 + x2$

وبالنسبة للشكل $GF(2^n)$، فإنه أيضا يمثل حلقة منتهية بالامكان حسابها كما في الشكل السابق.

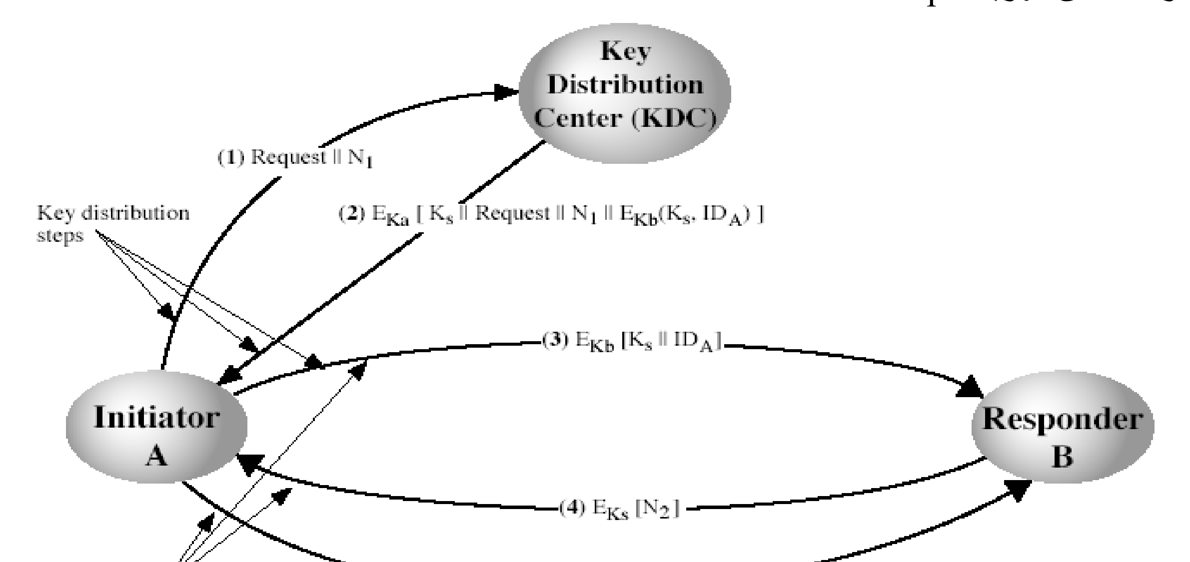
الفصل السابع: المصادقة بإستخدام التشفير المتماثل
Confidentiality Using Symmetric Encryption

Key Distribution توزيع المفاتيح

- في الطريقة التماثلية symmetric يشترك كل طرف في مفتاح سري عام.
- القضية هي كيفية توزيع هذا المفتاح بطريقة موثوقة.
- يفشل نظام الحماية عادة بسبب كسر عملية تبادل المفاتيح.
- توجد ثلاثة بدائل لتوزيع المفاتيح بين الطرفين أ و ب:
  ١. يولد أ المفتاح ويسلمه فيزيائيا إلى ب .
  ٢. طرف ثالث يختار المفتاح ويسلمه للطرفين.
  ٣. يمكن إستخدام مفتاح مشفر مستخدم في اتصال سابق، لتشفير مفتاح جديد.
  ٤. إذا كان الطرفان أ و ب يمتلكان إتصالا آمنا عن طريق طرف ثالث جـ، يمكن ان يقوم الطرف الثالث بعملية تبادل المفاتيح بين الطرفين أ ، ب.

- **سيناريو توزيع المفاتيح Key Distribution Scenario**

كما يوضح الشكل ادناه، فإن عملية توزيع المفاتيح تتم بخمس خطوات، الثلاث الخطوات الاولى بخطوات توزيع المفاتيح **Key Distribution**، اما الثلاث الاخيرة (الخطوة الثالثة مصنفة في الخطوتين) فتسمى بخطوات المصادقة، اوالتأكد من الهوية authentication steps .



Key Distribution Scenario

- **قضايا توزيع المفاتيح Key Distribution Issues :**

إن هيكلية التوزيع مطلوبة في الشبكات الكبيرة، لكن يفترض وجود ثقة متبالة بينها.
يجب ان يكون عمر دورة حياة جلسة توزيع المفاتيح session key محدودا من أجل امنية افضل في حالة كان النظام موثوقا .. فإنه بالامكان جعل جلسة المفاتيح مؤتمتة آليا.

الفصل الثامن : مدخل إلى نظرية الاعداد
Introduction to Number Theory

- الاعداد الأولية Prime Numbers :

هي اعداد صحيحة integer numbers لا تملك سوى قاسمين هم الواحد الصحيح والعدد نفسه مثلا الاعداد ٢,٣,٥,٧ اعداد اولية.
تشكل الاعداد الاولية مركز نظرية الاعداد.

- تحليل الاعداد الاولية إلى عواملها Prime Factorisation :
  - تحليل العدد n هو عملية كتابته على شكل ناتج مجموعة من الاعداد الصحيحة مضروبة مع بعضها n=a × b × c.
  - التحليل الاولي الى عوامل هو كتابة العدد على شكل اعداد اولية مضروبة مع بعضها مثلا :
    91=7×13 والعدد 3600=24×32×52
  - الاعداد الاولية النسبية Relatively Prime Numbers :

يمكن تعريف العددين الصحيحين انهما اوليان نسبيا (اوليان فيما بينهما) إذا كان العامل المشترك لهما هو الواحد فقط، مثلا العددين ٨ و ١٥ اوليان نسبيا وذلك لأن عوامل العدد ٨ هي (١,٢,٤,٨) و عوامل العدد ١٥ هي (١,٣,٥,١٥) مما يعني عدم وجود عدد مشترك بخلاف الواحد بينهما.

- نظرية فيرمات Fermat's Theorem:

تنص على انه إذا كان هناك عدد اولي p، وكان الـ GCD له مع عدد صحيح a يساوي واحد، أي أن a , p اوليان فيما بينهما أو اوليان نسبيا، فإن :

- a^{p-1} mod p = 1

تستخدم هذه النظرية في خوارزميات إنشاء المفتاح العام.

- دالة توشنت أولر Euler Totient Function ø(n) :

عند عمل إجراءات حسابية موديلو n، عدد عناصر هذه المجموعة هو n-1 من ٠ حتى العدد n-1، والمجموعة (المقلصة)/ المنقصة هي مجموعة الاعداد الاولية نسبيا مع n.
دالة أولر هي عدد العناصر الاولية نسبيا مع n، ويرمز لها بالرمز ø(n).

- ولحساب دالة اولر للعدد الصحيح n أو عدد الاعداد الاولية النسبية لـ n فإنه:

إذا كان n عدد اوليا فإن ø(n)=n-1 ،
وإذا كان n = p . q فإن ø(n)= ø(p.q)= (p-1)(q-1)
وهما الطريقتان التين اثبتهما اولر لحساب قيمة دالته، وذلك بالاستعانة بنظرية فيرمات.
مثال:

- ø(37) = 36 , (37 is a prime)
- ø(21) = (3–1)×(7–1) = 2×6 = 12 , (21= 3 * 7)

- نظرية اولر Euler's Theorem:

وقد ولد اولر نظرية اولر بتطبيق نظرية توشنت اولر على نظرية فيرمات، تنص نظرية أولر على:

- $a^{ø(n)}$mod N = 1 ,where GCD (a , N) = 1..

- مثالين على ذلك:

- *a*=3;*n*=10; ø(10)=4;
- hence 34 = 81 = 1 mod 10

- $a=2;n=11;\ ø(11)=10;$
- hence 210 = 1024 = 1 mod 11

الفصل التاسع: تشفير المفتاح العام و خوارزمية RSA
Public Key Cryptography and RSA

- تشفير المفتاح الخاص private Key Cryptography:

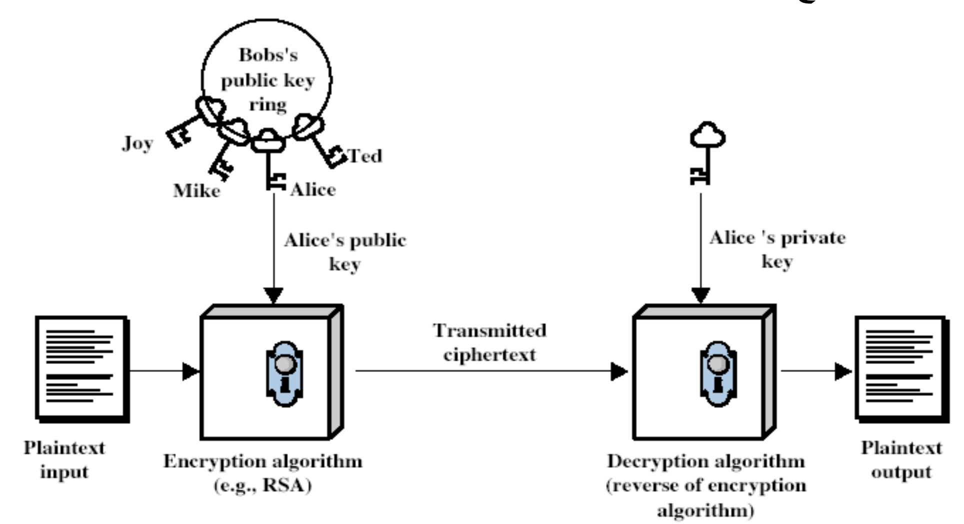
تستخدم هذه الطريقة مفتاح واحد للطرفين، إذا تم كشف طريقة الاتصال تم فضح هذه الرقم، ولا يحمي المرسل من تزييف المستقبل لرسالة والزعم انها من المرسل.

- تشفير المفتاح العام Public Key Cryptography :

تعتبر من افضل الطرق على مدى ٣٠٠٠ عام من تاريخ التشفير، تستخدم مفتاحين عام وخاص، تسمى بالتشفير الغير متماثل لأن الطرفين غير متطابقين، يستخدم تطبيقات قوية تعتمد على دوال نظرية الاعداد.
متكاملة بشكل افضل من التشفير بالمفتاح الخاص.

- تعريف التشفير بالمفتاح العام/بالمفتاحين/الغير متماثل public-key/two-key/asymmetric

هو طريقة تشفير تعتمد مفتاحين:
المفتاح العام KU : هو مفتاح قد يكون معلوما للجميع، ويستخدم لتشفير الرسائل وللتحقق من التوقيعات.
المفتاح الخاص KR : معروف فقط للمستقبل، يستخدم فقط لفك الشفرة، وللتوقيع/ إنشاء التوقيع .
وقد سمي بغير المتماثل asymmetric لأن هؤلاء الذين يشفرون او يفحصون التوقيع لا يستطيعون فك شفرتهم او إنشاء التوقيع نفسه.
الشكل ادناه يوضح هذه المنظومة.



- لماذا يتم استخدام طريقة المفتاح العام:

وذلك من اجل انجاز قضيتن هامتين هما:
- توزيع المفاتيح key distribution: كيف يمكن إلحصول على اتصال محمي/آمن بشكل عام، دون النظر في صوابية عملية توزيع المفاتيح.
- التوقيع الالكتروني digital signatures : كيفية ضمان وصول الرسالة نفسها بشكل سليم من الشخص المرسل.

- يعزى اختراع المفتاح العام إلى العالمين ديفي و هيلمان في جامعة ستانفورد في ١٩٧٦م.
- خصائص المفتاح العام :

إن خوارزميات توليد المفتاح العام تعتمد على الخصائص التالية:

١. العملية الحسابية لإيجاد فك الشفرة غير ممكنة عمليا، أو غير مجدية.
٢. عملية فك الشفرة ممكنة بالنسبة للطرف الذي يعرف المفتاح.
٣. اي من المفتاحين يمكنهما التشفير، ولا يفك الشفرة إلا الآخر.

- الشكل التالي يوضح منظومة التشفير بالمفتاح العام:

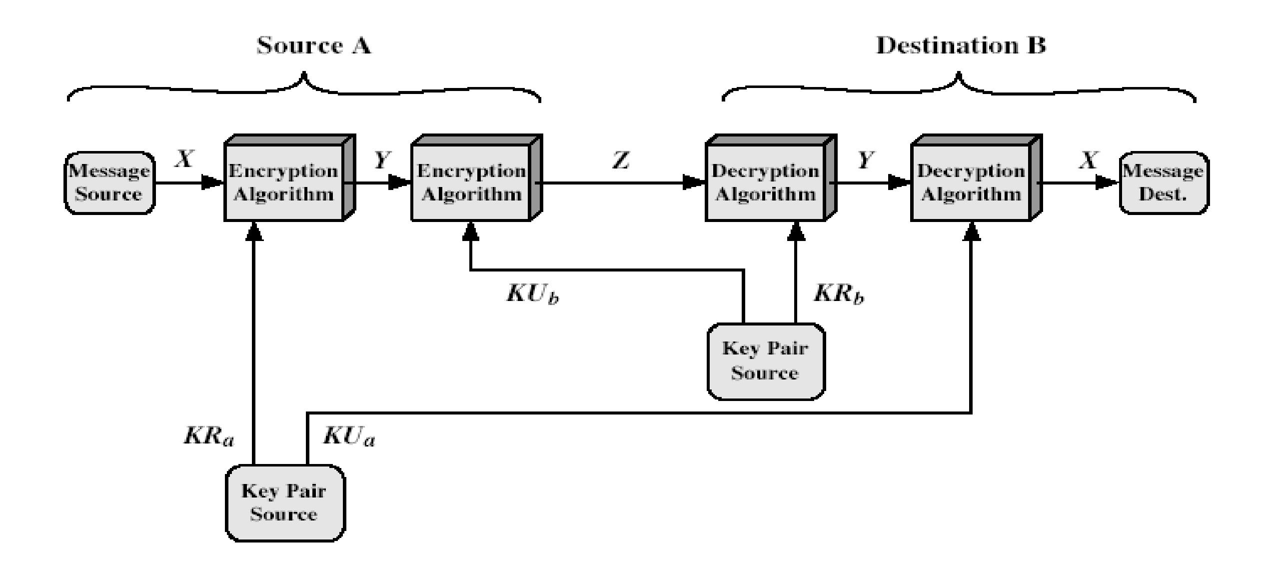


Figure 9.4 Public-Key Cryptosystem: Secrecy and Authentication

- تطبيقات طريقة المفاتيح العامة :

تطبق هذه الطريقة في ثلاثة طرق عامة تقريبا:
الاولى : التشفير وفك التشفير لإعطاء السرية.
الثانية : التوقيع الالكتروني لإعطاء المصداقية/ التصديق أو التأكد من الهوية.
الثالثة : تبادل المفاتيح وذلك اثناء جلسة المفاتيح.
بعض الخوارزميات تدعم كل هذه الاستخدامات، كما ان بعضها لا يدعم سوى واحدة.

- حدود السرية في أنظمة المفاتيح العامة:

ـ مثل المفاتيح الخاصة يستطيع المهاجم عمل بحث رياضي موسع وإيجاد المفاتيح من الناحية النظرية.
ـ ولذلك تستخدم اعداد كبيرة جدا كمفاتيح (اكثر من ٥١٢ بتا).
ـ تعتمد السرية هنا على الفجوة الكبيرة والمعقدة بين سهولة التشفيروفك التشفير مقابل صعوبة مسائل تحليل التشفير.
ـ بشكل عام فإن المسألة الصعبة مصدرها صعوبة تطبيق عملية إيجاد المفتاح عمليا في الواقع، ويشترط لذلك استخدام اعداد كبيرة جدا.
ـ وعلى هذا الاساس فإن التشفير الغير متماثل أبطء مقارنة بالتشفير المتماثل.

- خوارزمية RSA (رايفست، شامير، والديمان):

عام ١٩٧٧م قدمت وهي من اشهر الطرق في تطبيق التشفير التماثلي، تعتمد على الحقول المنتهية المرفوعة للقوى، والمطبقة على الاعداد الاولية، تستخدم اعداد كبيرة جدا مثلا (١٠٢٤بت)، تعتمد صعوبتها على تعقيد التحليل إلى عوامل بالنسبة للأعداد الكبيرة.

- شرح خوارزمية RSA:

يقوم كل واحد من طرفي الارسال والاستقبال بتوليد مفتاحه العام، وذلك بتنفيذ الخوارزمية التالية:

١. يختار عددين اوليين كبيرين عشوائيا وليكونا P و q.
٢. يتم حساب عدد الموديلو المستخدمN، وذلك بإيجاد ناتج ضربهما حيث:
$N = p . q$ مع ملاحظة ان ذلك يعني ان ($Ø (N) = (p - 1) (q - 1)$).
٣. يتم اختيار عدد عشوائيا كمفتاح خاص بشرط كونه اصغر من عدد الاعداد الاولية النسبية مع N، اي يكون العدد e اقل من $Ø (N)$ وبالطبع اكبر من الواحد الصحيح، وان يكون القاسم المشترك الاعظم للمفتاح e مع $Ø (N)$ هو الواحد الصحيح، اي ان يكون اوليا بالنسبة لـ $Ø (N)$. يرمز لهذا الشرط كالتالي:
where $1<e<ø(N)$, $GCD(e,ø(N))=1$)
٤. من اجل الحصول على مفتاح فك الشفرة يتم الحصول على العدد d، والذي نستطيع حسابه من العلاقة :
$e . d = 1 \mod ø(N)$ and $0 \le d \le N$

٥. يكون المفتاح العام مكونا من الصيغة KU={e,N}، حيث KU ترمز للمفتاح العام، الذي سوف يتم توزيعة بعد ذلك.
٦. يتم الاحتفاظ بشكل سري بالمفتاح الخاص، والذي يفك شفرة المفتاح العام، والمكون من الصيغة KR={d,p,q}، حيث KR ترمز للمفتاح الخاص.

- إستخدام الخوارزمية عمليا RSA Use

يقوم المرسل بتشفير الرسالة، ولتكن M وذلك بتطبيق المفتاح العام عليها KU={e,N}، لتنتج الرسالة المشفرة C وذلك بالصورة :

$C = M^e \bmod N$, where $0 <= M < N$.

إن الشرط المطبق على الرسالة M، يعني ان يطبق على القالب block الذي يتم تمريره على الخوارزمية من اجل تشفيرها.

إن فك شفرة الرسالة C، يتم في الواقع باستخدام المفتاح الخاص لصاحب المفتاح العام المستخدم في التشفير، واضح جدا ان مطبق عملية التشفير يعجز عن فك الشفرة وذلك لأن حساب قيمة دالة تيوشن اويلر(ø(N ، يتعقد كلما كبر العدد N، بينما مالك المفتاح الخاص يعلم ان الدالة (ø(N يمكن الحصول عليها بإستخدام العددين p,q، المكونان لصيغة المفتاح الخاص به.

يتكون المفتاح الخاص من KR={d,p,q}، وعن طريقه يستطيع المستقبل حساب قيمة M في الدالة:

$M=C^d \bmod N$

- تحليل خوارزمية RSA:

تعتمد هذه الخوارزمية على نظرية اويلر، التي تنص على ان :

$a^{ø(n)} \bmod N = 1$,where $GCD (a , N) = 1$.

وحسب الخوارزمية فنحن نملك:

$N = p . q$ and $ø(N) = (p – 1) (q – 1)$

يتم إذن إختيار e وبالتالي d ، بحرص حتى يتم عكسهما إعتمادا على موديلو ø(n) ((mod ø(n))، ولذلك فإن:

$e . d = 1 + k . ø (N)$,for some k

لأن e و d متعاكسان حسب الحقل المنتهي **(. , + , ø(N))**، ولذلك فإن:

$$C^d = (M^e)^d = M^{1+k.ø(N)} = M^1.(M^{ø(N)})^k = M^1.(1)^k = M^1 = M \bmod N$$

- مثال على الخوارزمية:

- Select primes: *p*=17 & *q*=11
- Compute *n* = *pq* =17×11=187
- Compute ø(*n*)=(*p*–1)(*q*-1)=16×10=160
- Select e *:* gcd(e,160)=1; choose *e*=7
- Determine d*: de*=1 mod 160 and *d* < 160 Value is d=23 since 23×7=161= 10×160+1
- Publish public key KU={7,187}
- Keep secret private key KR={23,17,11}

-

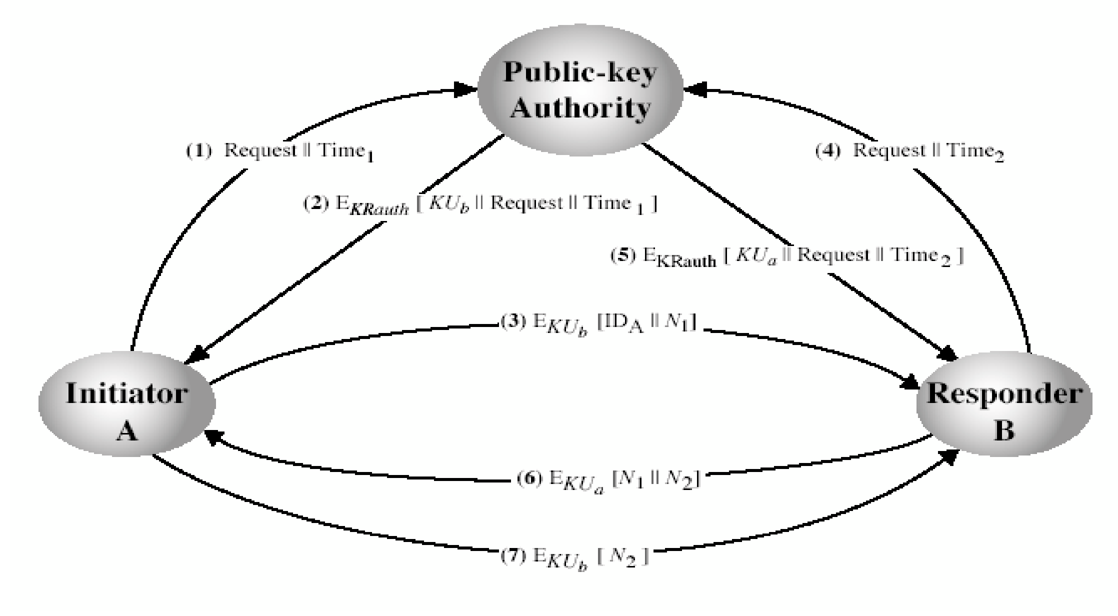
الفصل العاشر: إدارة المفاتيح، نظم تشفير اخرى للمفتاح العام
Key Management; Other Public Key Cryptosystems

- توزيع المفتاح العام Distribution of Public Keys:

يتم ذلك بعدة طرق هي:

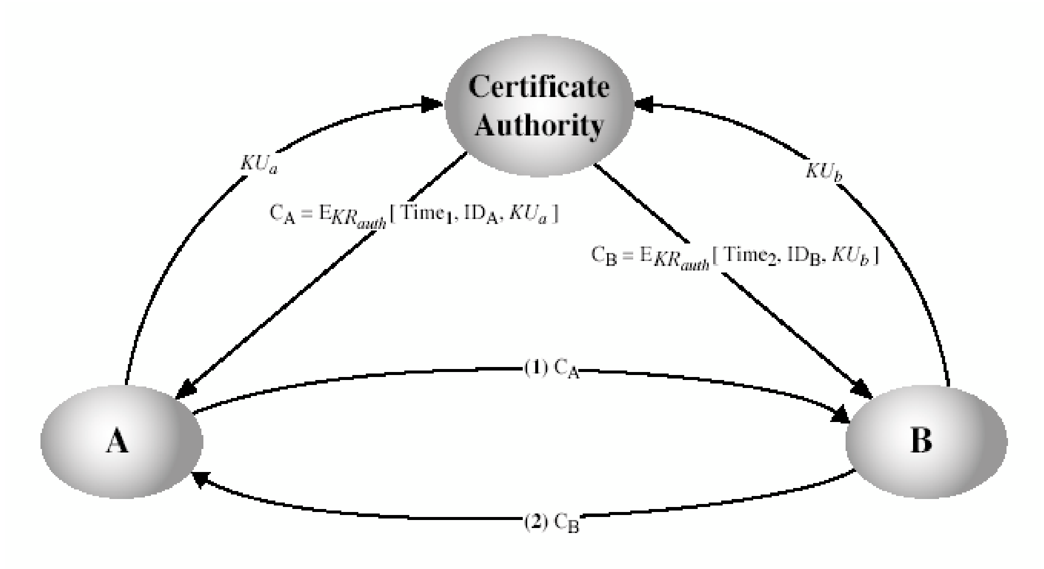
١. الاعلان العمومي Public announcement
٢. دليل عام متاح للجميع Publicly available directory
٣. هيئة المفتاح العام Public-key authority
٤. شهادات المفتاح العام Public-key certificates

١ـ الاعلان العام :
عملية اعلان المفتاح العام بواسطة البريد او الاذاعة او مجموعات الاخبار، وهذه الطريقة لها سلبيات هي سهولة التزييف، اي منتحل يستطيع عمل مفتاح عام وتوزيعه على الجميع كأنه جزء من المجموعة، وحتى يتم اكتشافه يستطيع الاستمرار بالتنكر بذلك.
٢ ـ دليل عام:
هي طريقة جيدة تستخدم من أجل توزيع خاص لذلك الدليل الذي يحتوي على المفاتيح العامة، ويجب ان يتميز بالخصائص التالية:
يحتوي على بيانات الاسم والمفتاح العام، يسجل فيه المشتركون اولا، يستطيع المشترك تغيير المفتاح في اي لحظة، يتم نشر الدليل بطريقة دورية، يتم الوصول إلى الدليل بطريقة الكترونية.
مازال الدليل عرضة للسطو من قبل المحتالين والمزيفين.
٣ ـ الهيئة الخاصة بتوزيع المفتاح العام:
كما يوضح الشكل ادناه، فهي طريقة اكثر انضباطا وتحكما من الدليل العام، تملك نفس الخصائص السابق ذكرها للدليل، بالاضافة إلى وجود مفتاح عام خاص بالهيئة/ الدليل، يتم التواصل بعد ذلك بالدليل (الهيئة) لطلب اي مفاتيح عامه، تحتاج إلى وصول فوري (real-time) مع الهيئة عند الاحتياج.



Public-Key Authority

٤ ـ شهادات المفتاح العام:
كما يوضح الشكل ادناه، فهذه الطريقة تجمع ميزات الطرق السابقة، بالاضافة إلى انها لا تجعلك تحتاج إلى ان تسابق الزمن من اجل الوصول إلى الهيئة الوسيطة! كما في الطريقة السابقة، يتم دمج الشهادة مع اسم التعريف للعضو مع المفتاح العام (احيانا مع معلومات اخرى اضافية)، ثم التوقيع على هذه الحزمة من قبل الهيئة التي تصدر الشهادات.



Public-Key Certificates

يقوم المرسل باستخدام هذه الشهادة التي تحتوي على هويته ومفتاحه العام، في عمليات التراسل مع طرف آخر، يملك معلومات مشابهة عن طريق هيئة اصدار الشهادات.

- توزيع المفاتيح العامة للمفاتيح الخاصة:

يتم استخدام الوسائل السابقة من اجل توزيع المفاتيح العامة وذلك لضمان السرية والتعرف على الهوية، ولكن خوارزميات المفتاح العام مازلت بطيئة، ولذلك فما زلنا نرغب في استخدام المفاتيح الخاصة من اجل تشفير محتوى الرسائل، ولهذا يتم استخدام جلسة توزيع المفاتيح (تستخدم فيه المفاتيح العامة لتشفير المفاتيح الخاصة، التي تستخدم بدورها لتشفير الرسائل المتبادلة)، هناك عدة طرق لتفنيذ جلسات توزيع المفاتيح هذه .

- الطريقة البسيطة لتوزيع المفاتيح Simple Secret Key Distribution

قدمت عام ١٩٧٩م بواسطة ماركل، يقوم المرسل بتوليد مفتاح عام يبدأ به الجلسة ....، ومن عيوب هذه الطريقة سهولة انتحال شخصية احد الطرفين من قبل المهاجم.

- طريقة ديفي ـ هلمان لتبادل المفاتيح Diffie-Hellman Key Exchange

من اول النظم المقدمة لتوزيع المفاتيح، في عام ١٩٧٦م بواسطة العالمين ديفي وهلمان، وهي طريقة عملية لتوزيع المفاتيح، وتستخدم حاليا على نطاق واسع في المجال التجاري.

- نظام توزيع المفاتيح العامة في هذه الطريقة :
  - ← لا يمكن استخدامه ـ نظرا لتعقيده ـ في التراسل العادي بالرسائل.
  - ← تستخدم فقط لإنشاء جلسة توزيع مفاتيح عامة.
  - ← معروفة فقط للمشتركين الاثنين ، المرسل والمستقبل.

قيمة المفاتيح تعتمد على المشتركين، وعلى المعلومات المحتواة للمفاتيح العامة والخاصة.

تعتمد هذه الطريقة على الرفع للقوة، في الحقول المنتهية (حقل جلويس)، موديل عدد اولى او كثيرة حدود ـ وهي طريقة سهلة للتوليد.

تعتمد سرية هذه الطريقة على صعوبة حساب اللوغاريتم المتقطع، (عملية عكس الرفع للاس)، وهي معقدة بشكل مشابه للتحليل إلى عوامل في طريقة (RAS)، وهي مسألة معقدة.

- يتفق الطرفان على مجموعة من البارمترات العامة هي :

إختيار عدد صحيح اولي (او كثيرة حدود)، q مثلا.

إختيار α جذر اصلي/صحيح موديلو q.

يقوم كل طرف بتوليد المفتاح الخاص به، بإختيار عدد صحيح اقل من q (مثلا المرسل A يقوم باختيار العدد x_A ، $x_A<q$)، وعن طريقه يحسب المفتاح العام y_A بالقانون $(y_A = \alpha^{x_A} \bmod q)$.

- فإذا كان المفتاح المختار للمرسل A هو y_A وللمستقبل B هو y_B فإن جلسة تبادل المفاتيح تكوّن K_{AB} حيث:

$K_{AB} = y_A\ y_B \bmod q = \alpha^{xA.xB} \bmod q$ (حسب التعريف)

$K_{AB} = y_A^{xB} \bmod q$ (which **B** can compute) وهذه الصيغة للحساب لدى المستقبل

$K_{AB} = y_B^{xA} \bmod q$ (which **A** can compute) وهذه الصيغة للحساب لدى المرسل

يستخدم المفتاح العام K_{AB} فقط في جلسة تبادل المفاتيح من اجل تشفير المفتاح الخاص/السري.

بإمكان الطرفين عمل جلسة تبادل مفاتيح جديدة، لتغيير المفتاح العام او المفاتيح الخاصة.

يحتاج المهاجم إلى الحصول على أحد العددين x_A و x_B حسب الطرف الذي يرغب في مهاجمة رسائله، وهو ما يكلفه مجموعة من عمليات اللوغاريتم المتقطع كما اسلفنا.

- مثال على طريقة ديفي ـ هلمن لتوزيع المفاتيح :

لنفترض ان الطرفين A و B قد اتفقا على العددين q و α كالتالي :

$q=353$, $\alpha=3$

يقوم A بإختيار عشوائيا عدد صحيح اقل من q وليكن $x_A=97$، و B يختار $x_B=233$ ..

لنحسب المفاتيح العامة لكل طرف كالتالي :

(A) $y_A=397 \bmod 353 = 40$

(B) $y_B=3233 \bmod 353 = 248$

فيكون المفتاح المشترك في جلسة المفاتيح وهو K_{AB} كالتالي:

(A) $KAB= y_Bx_A \bmod 353 = 24897 \bmod 353 = 160$

(B) $KAB= y_Ax_B \bmod 353 = 40233 \bmod 353 = 160$

نفس الرقم ولكنه يحسب بطريقة مختلفة من جهة كل طرف، حسب المعلومات (المفتاح الخاص) الموجودة لديه.

الفصل الحادي عشر: التحقق من هوية الرسالة، ودوال المربع/ الهاش
Message Authentication and Hash Functions

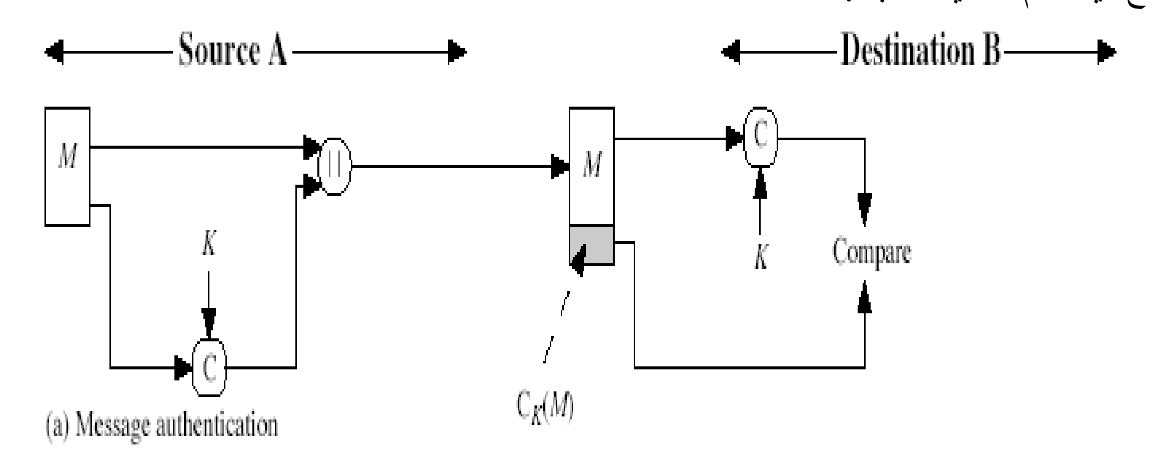
- كود التحقق من هوية الرسالة Message Authentication Code (MAC) :

تقوم خوارزمية معينة بتوليد قالب/وحدة بتات صغير ذا حجم ثابت، وذلك بالاعتماد على كلا من محتوى الرسالة ومجموعة مفاتيح، وبشكل مشابه للتشفير لا يفترض ان يستطيع الماهجم فك شفرة هذا القالب.

يتم دمج هذا الكود الـ(MAC) مع الرسالة كأنه توقيع.

يقوم المستقبل للرسالة بإجراء نفس العمليات على الرسالة، ويقارن نتائجه بالكود المرفق، فإذا كان الكود MAC الذي ولده المستقبل يطابق الكود المرفق، فهذا يعني سلامة الرسالة، وأنها وصلت من نفس المرسل.

الشكل التالي يوضح كيف تتم العملية السابقة.



(a) Message authentication

- وكما يوضح الشكل فإن هذا الكود المدمج يقدم لنا ما يسمى بالمصادقة او المصداقية confidentiality
- ويمكن ان يستخدم مع التشفير، رغم ان هذا الاجراء منفصل تماما عن عملية تشفير الرسالة المذكور سابقا.
- ومع ذلك فيمكن ان يتم إجراء حساب هذا الكود قبل تشفير الرسالة او بعدها. ويفضل عادة ان يتم ذلك قبل تشفير الرسالة، بحيث يتم التأكد من مصادقة الرسالة بعد فك شفرتها.
- أحيانا تكون المصداقية اوالمصادقة هي المطلوبة فقط .. فيتم استخدام الـ MAC.
- احيانا يكون هناك احتياج آخر للمصادقة بـ MAC بعيدا عن قضايا التشفير، (كالارشفة مثلا).
- من الجدير ملاحظته ان كود الـ MAC الموضح هنا ليس هو التوقيع الالكتروني digital signature الذي سوف يأتي لاحقا.

- خصائص الكود MAC:
- يعتبر الماك عملية حساب وثيقة البيانات المرسلة ما يسمى بالـ checksum :

MAC = CK(M) , where M is the message

- يقوم الماك بإيجاز وتلخيص الحجم المتغير للرسائل المختلفة.
- يستخدم طريقة المفتاح الخاص المعروفة.
- يستخدم كحجم ثابت للموثق للمصادقة to a fixed-sized authenticator.
- يعتبر دالة من النوع (كثير إلى واحد) أو many-to-one function.
- لا يفترض ان تكون لمجموعة من الرسائل نفس الماك، ووجود ذلك يجب ان يكون غاية في الصعوبة.

- متطلبات كود الـ MAC:

يجب الاخذ في الاعتبار مختلف انواع الهجمات المحتملة، يجب ان يكون كود الـ MAC محققا للتالي:

١) بمعرفة الرسالة والماك الخاص بها، يصعب بشكل كبير (غير مجدي) الحصول على رسالة لها ذات الماك.
٢) يجب توزيع اكواد الماك بشكل مطرد/منتظم، مع كل رسالة.
٣) يجب ان يعتمد كود الماك على جميع (بتات) الرسالة.

- إستخدام التشفير المتاثل من اجل كود الماك:

يمكن تطبيق اي سلسلة من قوالب التشفير على ان يكون الماك هو القالب الاخير.

خوارزمية مصادقة البيانات Data Authentication Algorithm (DAA) هي الخوارزمية التي تنفذ كود الماك بالاعتماد على خوارزميات التشفير القديمة للمفتاح الخاص مثل DES-CBC.

تستخدم هذه الخوارزمية الصفر كقيمة ابتدائية، وكذلك كقيم مكملة للفراغات النهائية في القالب ما يسمى بالـ (zero-pad of final block)،التشفير يكون باستخدام خوارزمية الـ DES بنمط الـ CBC، وحجم الماك يكون القالب الاخير او البتات الابعد من جهة اليسار في الرسالة.

ولكن كود الماك الحاصل من استخدام هذه الخوارزمية لا يحقق الحجم المطلوب لتحقيق الامنية.

- تقنية الدالة المربعة/الهاش Hash Functions :

تنجز عملية تكثيف الرسالة بطريقة اعتباطية إلى حجم ثابت محدد لكل رسالة، ويتم الافتراض ان دالة الهاش هي دالة عامة وليست مفتاحا، تستخدم اذن لاكتشاف التغيرات الطارئة على الرسالة قبل وصولها، يمكن تطبيقها بطرق متعددة على الرسالة، غالبا تستخدم بعد ذلك لانشاء التوقيع الالكتروني.

- خصائص دالة الهاش Hash Function Properties :
- تنشئ دالة الهاش ما يشبه بصمة اصبع الابهام، للملفات او الرسائل او البيانات:

h = H(M)

- تختزل الاحجام المختلفة للرسائل M إلى بصمة الابهام ثابتة الحجم.
- يفترض ان تكون عامة، متاحة للجميع.

- متطلبات تنفيذ دالة الهاش Requirements for Hash Functions :

١. تكون قابلة للتطبيق على اي رسالة بأي حجم.
٢. مخرجاته ثابتة من حيث عدد البتات الحجم.
٣. سهلة الحساب بالنسبة لأي رسالة M، بالشكل العام h = H(M) .
٤. والحصول على h لا يساعد على الحصول على M حسب الدالة اعلاه. (خاصية الطريق الواحد)
٥. إذا كان H(y)=H(x) حسب شكل دالة الهاش، فإن الحصول على x لا يعني مطلقا القدرة على إيجاد y.
٦. إذا كان H(y)=H(x) فإنه من غير المجدي الحصول منها على x ولا y.

١٢	**MD5,SHA-1 full**
١٣	**٤-٥-٦-٧-٩-١٠-١١-١٢-١٣- DSS- ١٧ -١٨-١٩-٢٠**
١٤	**Kerbrose5**
١٥	**محذوف**
١٦	
١٧	**١٣-١٤-١٥-١٦-١٧-١٨-١٩-٢٠-٢١**

الفصل الثاني عشر: خوارزميات الهاش Hash Algorithm

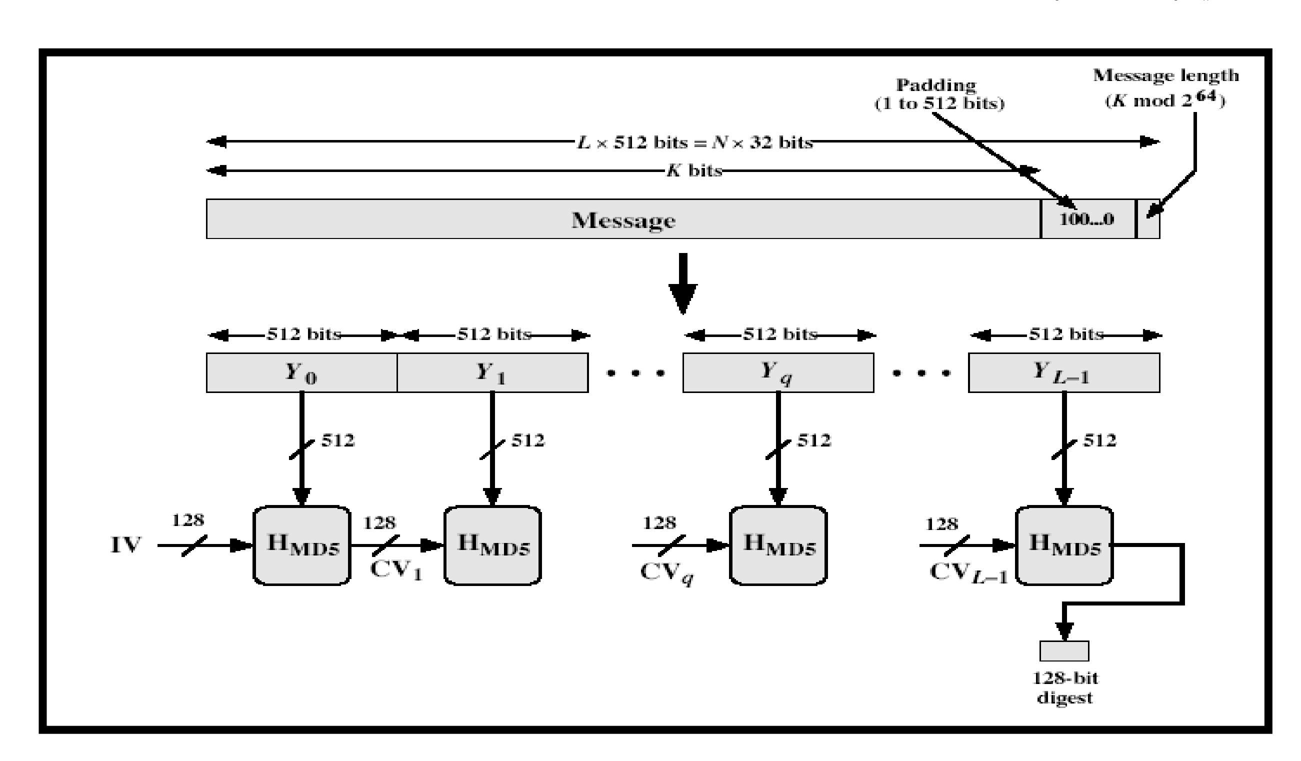
قدمت خوارزميات الهاش الكثير من الميزات منها:

- افضل انواع التشفير بالقالب block cipher
- زيادة قوة مقاومة الهجمات من النوع brute-force، والتي يقوم اصحابها بإجراء عمليات حسابية لفك شفرة الرسالة plaintext.
- لها انواع كثيرة منها: MD4 , MD5, SHA-1 , RIPEMD-160
- وكما يحدث في التشفير بالقالب، تستخدم الطرق التركيبية.

خوارزمية (تلخيص الرسالة) message digest MD5:

- صممت بواسطة رايفست وهو احد الثلاثة الذين ابتكروا خوارزمية الـ RAS.
- آخر اشكال مجموعة خوارزميات MDn بعد MD2 و MS4.
- تنتج دالة هاش بقيمة (بحجم) ١٢٨ بتا.
- تعتبر حتى الوقت الحالي الخوارزمية الاكثر استخداما من خوارزمية دوال الهاش.
- يمكن الاستفسار عنها في النت عبر الاستعلام (RFC 1321).
- **طريقة عمل الـ MD5:**

- تحول حجم الرسالة إلى احد مضاعفات الـ ٥١٢ بتا، وذلك عن طريق الـ padding ويتم ذلك بإضافة أصفار إلى الحجم الاصلي للرسالة حتى تكون من مضاعفات الـ ٥١٢ بت، على ان يخصص البت الاخير لقيمة الحجم الاصلي للرسالة.
- في الحافظة buffer الخاصة بالـ MD5، يتم عمل قيمة ابتدائية حجمها ١٢٨بت، على صورة اربعة كلمات هي (A,B,C,D).



MD5 Overview

- وعلى ذلك يكون القالب الواحد من الرسالة مكونا من ١٦ كلمة، لأن حجم القالب كما ذكرنا هو ٥١٢ بتا، يتم إدخال هذه الأجزاء الـ ١٦ إلى دالة الضغط (compression function)، وذلك نفس الوقت مع القيمة الابتدائية الجاهزة في الحافظة والتي حجمها ١٢٨ بتا.
- ينتج من دمج القيمة الابتدائية للحافظة buffer مع القالب الاول قيمة جديدة بطريقة معينة، يكون حجمها نفس حجم القيمة الابتدائية (IV0: initial value) وهو ١٢٨ بتا، يتم ادخالها في دالة ضغط أخرى مع القالب

الثاني من الرسالة بنفس الطريقة السابقة، حتى تنتهي قوالب الرسالة (مهما كان عددها، حسب حجم الرسالة نفسها).

- بهذه الطريقة يكون مخرجات العملية بالكامل كما هو موضح بالشكل أعلاه، عبارة عن قالب واحد بحجم ١٢٨ بت تعتبر خلاصة (digest) خوارزمية الـ MD5، يتم إلحاقها بالرسالة الممدة pad message.
- يقوم الطرف المستقبل عندئذ بتنفيذ نفس العمليات السابقة على الرسالة، ويقارن الناتج بالخلاصة (digest) المرفقة فإذا كانتا متطابقتين، ضمن سلامة (integrity) المحتوى.

دالة الضغط MD5 Compression Function:

هي الدالة التي تستقبل مدخلات القيمة الابتدائية اولا مع القالب الاول من الرسالة، وتسمى بالدورة الاولى round1، اما الدورة الثانية round2 فتستقبل مخرجات الدورة الاولى ١٢٨ بت ، وهكذا حتى الدورة الاخيرة التي تخرج لنا الخلاصة النهائية.

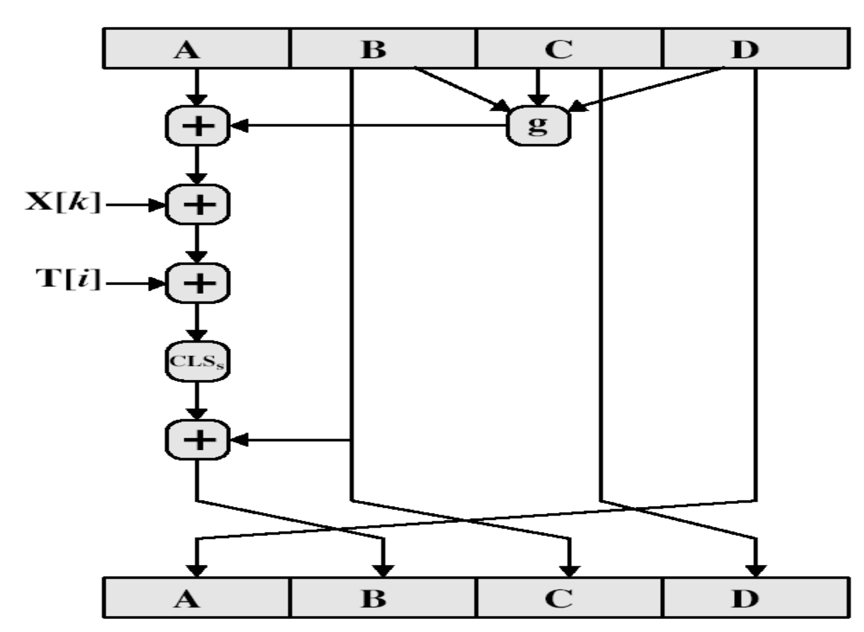
كل دورة من دورات تطبيق دالة الضغط تملك ١٦ خطوة من الشكل:

$$b=b+((a+ g(a,c,d) + X[k] + T[i])$$

حيث a,b,c,d هي الكلمات الاربع في الحافظة، لكنها تستخدم بعد إجراء بعض عمليات التباديل الرياضية عليها، بعد الخطوات الست عشر تكون الكلمة قد بدلت او حدثت ٤ مرات.

اما الدالة g(a,c,d) فهي دالة غير خطية متغيرة في كل دورة، اي انها في الدورة الاولى بالصيغة g، ولكنها في الدورات التالية تتغير من الشكل (f,g,h,i).

وكما يوضح الشكل ادناه، تحتوي كل دورة من ١٦ خطوة تطبق على الحروف الاربعة بالاضافة المدخلين x[k] و الدالة T[i] التي تشكل قيمة ثابتة مشتقة من دالة الجيب sin.



MD5 Compression Function

قوة خورازمية الـ MD5:

- تعتمد على جميع البتات المكونة للرسالة.
- يدعي رايفست مخترع الخوارزمية انها تقدم افضل أمنية ممكنة.
- ولكنها مع ذلك تعرضت لمجموعة من الهجمات الشهيرة، اي انها قابلة للإختراق.

خوارزمية الهاش الآمنة Secure Hash Algorithm (SHA-1):

- في البداية تم تصميم خوارزمية SHA بواسطة معهد NIST & NSA في عام ١٩٩٣م، ومن ثم تم مراجعتها في عام ١٩٩٥م لتخرج بالاسم الجديد SHA-1.
- تعتبر المقياس الامريكي للاستخدام مع نظام التواقيع DSA.
- تقدم عصارة/خلاصة رسالة بحجم ١٦٠ بت.
- حاليا هي الخوارزمية المفضلة لتطبيق الهاش.

- اعتمد تصميمها على خوارزمية الـ MD4، مع بعض الاختلافات.

عمل خوارزمية الهاش الامن SHA-1:

- كما في الـ MD5 تضيف هذه الخوارزمية padding ليكون حجم الرسالة من مضاعفات ٥١٢بت.
- تستخدم ٥ كلمات بحجم (١٦٠ بت)، في الحافظة التي تخزن القيمة الابتدائية initial value .
- العمليات التي تنفذ على شكل دورات ، تستخدم بعد القيمة الابتدائية المكونة (من ٥كلمات)، ١٦ كلمة طولها ٥١٢ بت:
  - توسع هذه الـ ١٦ كلمة إلى ٨٠ كلمة، عن الطريق المزج والتبديل (mixing & shifting).
- تضيف المخرجات من كل دورة إلى التالية لتكوين حافظة buffer جديدة.
- الحافظة الاخيرة التي تحمل المخرجات النهائية، هي قيمة الهاش المستخلصة.

دالة الضغط في SHA-1:

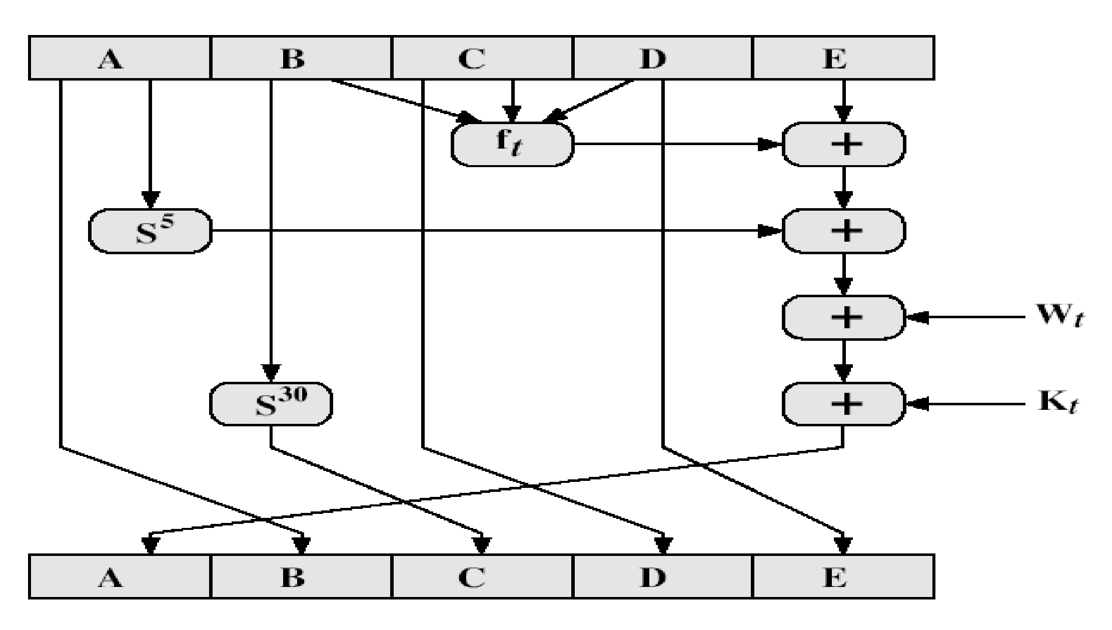
الفارق الرئيس بين الطريقتين (MD5) و (SHA-1) هو في تنفيذ دالة الضغط، وتعتمد دالة الضغط على عمليات تغيير قيم الحروف من القيمة الابتدائية (التي تمزج مع اول قالب من الرسالة) إلى الحصول على القيمة النهائية.

كل دورة تتكون من عشرين خطوة تقوم كل خطوة بإجراء عمليات تبديل للحافظات الخمس 5 buffers، حسب القاعدة:

$$(A,B,C,D,E) <-(E+f(t,B,C,D)+(A<<5)+W_t+K_t),A,(B<<30),C,D)$$

حيث ان a,b,c,d تعود للكمات الاربع المشابهة للخوارزمية السابقة، و t هي رقم الخطوة المطبقة في المرة الواحدة.

اما الدالة f(t,b,c,d)، فهي دالة غير خطية للدورة، و w_t فهي دالة مشتقة من قالب الرسالة المدخل في كل دورة، و k_t فهي قيم ثابتة مشتقة من دالة الجيب المعروفة، من اجل مزيد من التعقيد.



SHA-1 Compression Function

مقارنة بين الخوارزميتين (SHA-1 vs. MD5):

- الهجوم الشهير المعروف بالاسم brute force يكون في SHA-1 اقل اثرا منه في MD5 بسبب تعقيد الاحتمالية في الثانية (١٦٠ بتا مقابل ١٢٨ في الاولى).
- مقارنة بـالاولى فإن الخورازمية الثانية لم تتعرض لهجمات كثيرة ناجحة.
- رغم ذلك فإن الخوارزمية الثانية اكثر بطء (كمعالجة حاسوبية) من الاولى (بسبب تعقيدها: حيث يتم تنفيذها في ٨٠ خطوة مقابل الاولى MD5 التي تتم ب ٦٤ خطوة).
- كلا الخوارزميتين صممتا بشكل بسيط ومدمج.

Digital signature and authentication protocols

خصائص بنية التوقيع الرقمي :

١. يجب ان تعتمد على توقيع الرسالة، الضامن لسلامتها كالـ MAC مثلا.
٢. يجب ان تستخدم معلومات وحيدة للمرسل وذلك لمنع التزييف من جهة المهاجمين، والانكار من جهة المرسل او المستقبل.
٣. يجب ان تكون سهلة الانتاج نسبيا.
٤. يجب ان تكون وبصورة نسبية ايظا، سهلة التعرف والفحص للمقارنة.
٥. كذلك يجب ان تكون (غير مجدية infeasible) بالنسبة لإعادة حوسبتها من قبل المزورين، وذلك في حالتين هما:
   i. حالة انشاء رسالة جديدة مزيفة والتوقيع عليها.
   ii. حالة كسر التوقيع بالنسبة لرسالة اصلية موقع عليها مسبقا.
٦. يجب ان يكون من الممكن عمليا تخزين التوقيع الالكتروني فيزيائيا.

آلية التوقيع الرقمي:

عملية مختصة بين المرسل والمستقبل.
تفترض ان يملك المستقبل المفتاح العام الذي للمرسل.
يتم التوقيع عن طريق المرسل بواسطة مفتاحه الخاص، وذلك بتطبيق نفس فكرة الهاش التي تعتمد على احتواء جميع بتات الرسالة (بصورة مضغوطة) في التوقيع.
يمكن بالاضافة إلى ذلك تشفير الرسالة نفسها بواسطة المفتاح العام للمستقبل.
من المهم التوقيع اولا، ومن ثم تشفير الرسالة مع التوقيع بعد ذلك.
تعتمد سرية التوقيع وأمنيته اساسا على المفتاح الخاص للمرسل.

الوسيط في التوقيع الرقمي:

يتم الاستعانة بوسيط arbiter وليكن اسمه A:
يقوم الوسيط بالتحقق من أي رسالة موقعة.
يؤرخ الرسالة في حال سلامة التوقيع، ثم يوجهها إلى المستقبل.
نحتاج بالتأكيد إلى مستوى معين من الثقة في هذا الوسيط.
يمكن تنفيذ ذلك اما بمفتاح عام ، او مفتاح خاص.
يمكن ايظا ان نسمح له برؤية محتوى الرسالة، ويمكن ان لا يخول هذه الصلاحيات.

بروتوكولات المصادقة على الهوية:

تستخدم لعمليات قبول/التعرف الشركاء لهويات بعضهم البعض، ومن أجل جلسات تبادل المفاتيح.
يمكن ان تنفذ بطريقة (الطريق الواحد) او بطريقة تبادلية.
من القضايا الاساسية هنا وجوب وجود السرية لحماية الجلسة، وتحديد الزمن من اجل تجنب حصول المهاجم على وقت كافي يساعده في الرد بدلا من احد الطرفين.
المهاجم حين يرد بدلا من الطرف المتوقع ان يرد، تحدث مجموعة من الاحتمالات ويمكن تجنبها بـ:
إستخدام مجموعة من الاعداد المتسلسلة والمولدة بطريقة عشوائية.
إستخدام طابع الوقت، يحتاج إلى ساعة تزامن.
التحدي/ الاستجابة للتحدي تحتاج إلى استخدام نظام موحد في التعامل.

إستخدام التشفير التماثلي Using Symmetric Encryption :

كما هو واضح يمكننا استخدام مستويين لهيكلة للمفاتيح.
غالبا بواسطة مركز توزيع المفاتيح KDC الذي يكون موثوقا بالطبع:
كل طرف يشترك بمفتاح اساسي مع الـ KDC للتراسل.
KDC تولد جلسة مفاتيح تستخدم للاتصال بين الشركاء.
تستخدم المفاتيح الرئيسية master keys من اجل توزيع هذه المفاتيح بين الشركاء.

بروتوكول نيدهام-سكرويدر:

بروتوكول توزيع المفاتيح الذي يمثل الطرف الثالث الاصلي.

من اجل جلسة تبادل مفاتيح بين A و B، عبر الوسيط KDC.

فكرة عن البروتوكول:

1. A→KDC: ID_A || ID_B || N_1

2. KDC→A: E_{Ka}[Ks || ID_B || N_1 || E_{Kb}[Ks||ID_A]]

3. A→B: E_{Kb}[Ks||ID_A]

4. B→A: E_{Ks}[N_2]

5. A→B: E_{Ks}[f(N_2)]

يستخدم البروتوكول لتوزيع آمن في جلسة المفاتيح بين الطرفين.

نقطة ضعف وحيدة هي إحتمال الرد بواسطة المهاجم، في حالة انتهاك احدى الجلسات القديمة.

طرق الحالة كما ذكرنا سابقا تعتمد فكرة (ختم الوقت، طابع الوقت) أو نظام موحد في التعامل.

التوقيع الرقمي القياسي digital signature standard DSS:

الحكومة الامريكية قدمت هذه الطريقة لنظام التوقيع.

وذلك باستخدام خوارزمية الهاش الآمنة SHA.

في بداية التسعينيات صممت بواسطة NIST&NSA.

تنشئ هذه الطريقة ٣٢٠ بت كتوقيع، ولكن ضمن رقم سري حجمه من ٥١٢ إلى ١٠٢٤ بت.

تعتمد فكرة الطريقة على صعوبة الحساب المنفصل للوغاريتمات.

توليد مفاتيح الـ DSA Key Generation DSA :

وجود مفتاح عام مشترك قيمته (p,q,g):

حيث p عدد اولي كبير الحجم من الصورة : $p= 2^L$.

حيث L عدد بين ٥١٢ و ١٠٢٤ بت.

يتم اختيار q من ١٦٠ بت، كعدد اولي، من معاملات العدد p-1.

يتم اختيار g حيث :

$g = h^{(p-1)/q}$ where $h<p-1$, $h^{(p-1)/q} \pmod p > 1$

يختار المستخدم لنفسه مفتاحا خاصا x ليقوم بتوليد المفتاح العام y :

على ان يكون:

- $x<q$ و
- $y = g^x \pmod p$

عملية انشاء التوقيع الرقمي :

يتم توقيع الرسالة M بواسطة المرسل:

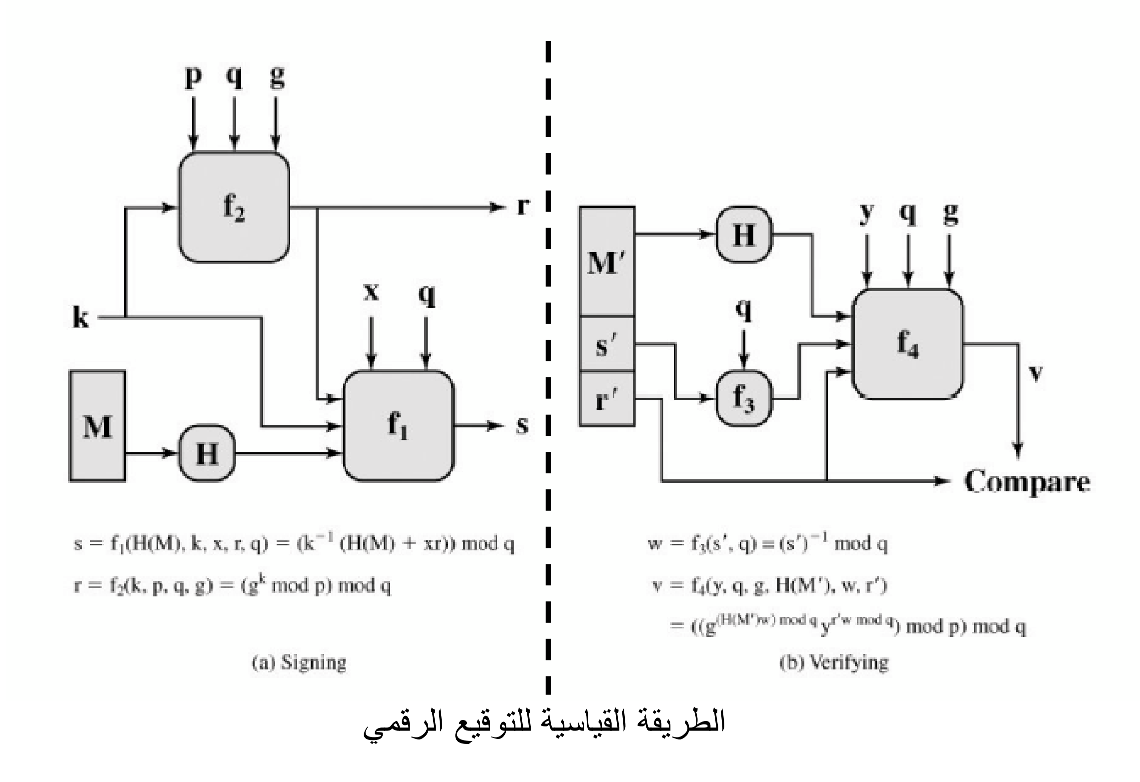
ينشئ المرسل مفتاح توقيع عشوائي k، بحيث k<q.

ثم يحسب زوجي التوقيع r,s حيث:

$r = (g^k \pmod p)) (\bmod q)$

$s = (k^{-1} .SHA (M) + x.r) (\bmod q)$

يقوم المرسل بعد ذلك بإرسال التوقيع (r,s) مع الرسالة M.



$s = f_1(H(M), k, x, r, q) = (k^{-1}(H(M) + xr)) \bmod q$

$r = f_2(k, p, q, g) = (g^k \bmod p) \bmod q$

$w = f_3(s', q) = (s')^{-1} \bmod q$

$v = f_4(y, q, g, H(M'), w, r') = ((g^{(H(M')w) \bmod q}\, y^{r'w \bmod q}) \bmod p) \bmod q$

الطريقة القياسية للتوقيع الرقمي

عملية التحقق من التوقيع DSA Signature Verification :

يقوم المستقبل بالفصل بين الرسالة M وجزئي التوقيع r و s .

من اجل عملية التحقق يقوم المستقبل بالحسابات التالية (كما في الشكل اعلاه):

$w = s^{-1}(\bmod q)$

$u1= (SHA(M).w)(\bmod q)$

$u2= (r.w)(\bmod q)$

$v = (g^{u1}.y^{u2}(\bmod p)) (\bmod q)$

- if v=r then signature is verified

ويطابق المستقبل بعد ذلك بين قيمة r التي وصلته مع الرسالة، وقيمة v التي حسبها اعلاه، فإذا كانتا متطابقتين كان هذا يعني ان عملية التحقق ناجحة.

قد يحتاج الباحث إلى إثبات ان r و v متطابقتين، ويوجد لذلك برهان رياضي كامل.

الفصل الرابع عشر : تطبيقات التحقق من الهوية

Authentication Applications

طريقة كربروس KERBEROS:

طريقة موثوقة من اجل نظام خدمة المفاتيح من المعهد الامريكي **MIT**.

تقدم لنا خدمة مصادقة مركزية للمفتاح الخاص ـ كطرف ثالث، عبر الشبكات الموزعة.

تسمح للمستخدمين الوصول للخدمات الموزعة عبر الشبكة.

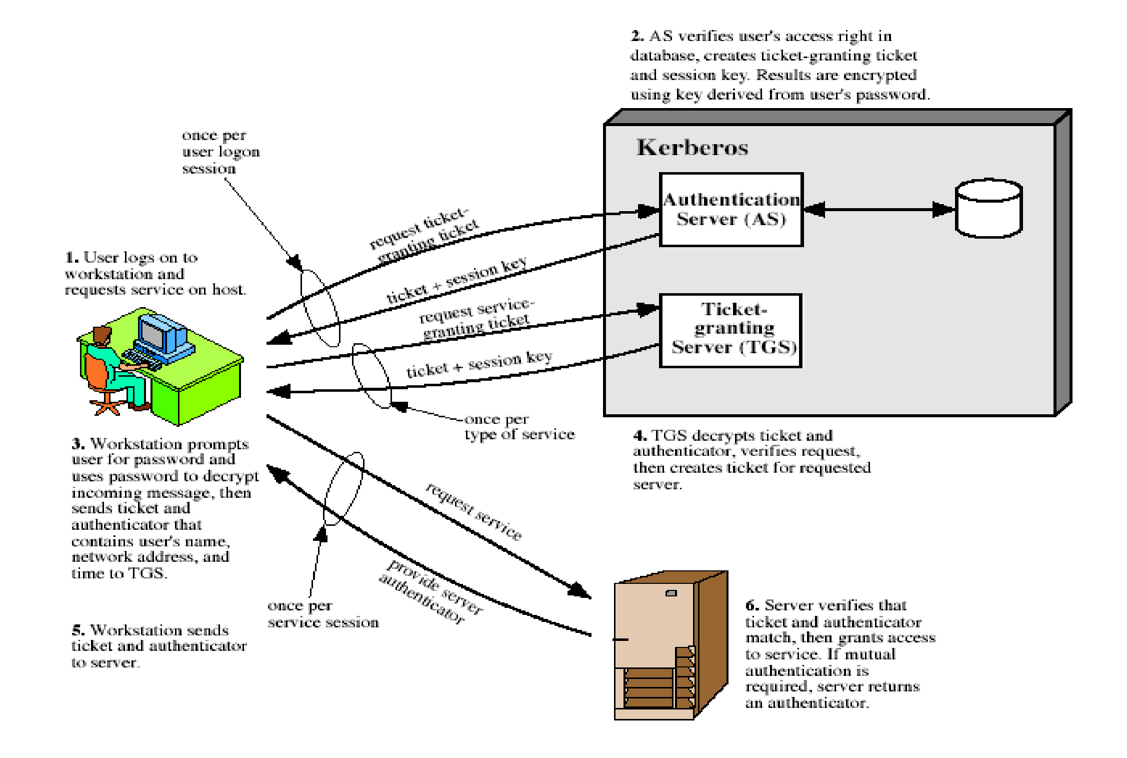
وذلك دون الحاجة إلى موثوقية كل محطات العمل.

توجد نسختين من هذه الطريقة هما : KERBEROS 4 و KERBEROS 5

متطلبات طريقة كيربروس:

- الامنية.
- الموثوقية.
- الشفافية.
- القابلية للتوسع.

يتم تنفيذها عبر بروتوكول المصادقة يعتمد على طريقة نيدهام-سكرويدر.



النسخة الخامسة من كربروس Kerberos Version 5 :

الرسمة أعلاه توضح العمليات المنفذة على هذه الطريقة، بالاضافة إلى التالي:

ـ طورت في منتصف التسعينيات.

ـ قدمت تطورات عن النسخة الرابعة هي:

عالجت نقص البيئة بـ:

ـ خوارزميات تشفير، بروتوكولات الشبكات، ترتيب البايت، دورة حياة التذكرة، تقديم المصادقة وغيره.

وكذلك النقص التقني بـ:

ـ التشفير المزدوج، نمط الاستخدام الغير قياسي، جلسة المفاتيح، هجمات كلمات المرور.

ـ على النت يمكن الاستفسار عنها بـ **RFC 1510**.

خوارزمية كربروس ٥ :

1) C → As : IDc || Pc || IDv .

2) As → C : Ticket.

3) C → As : IDc || Ticket.

where:

Ticket = E_{kv}[IDc || ADc || IDv]

C = client

As = server of authentication

IDc = identifier of user on C

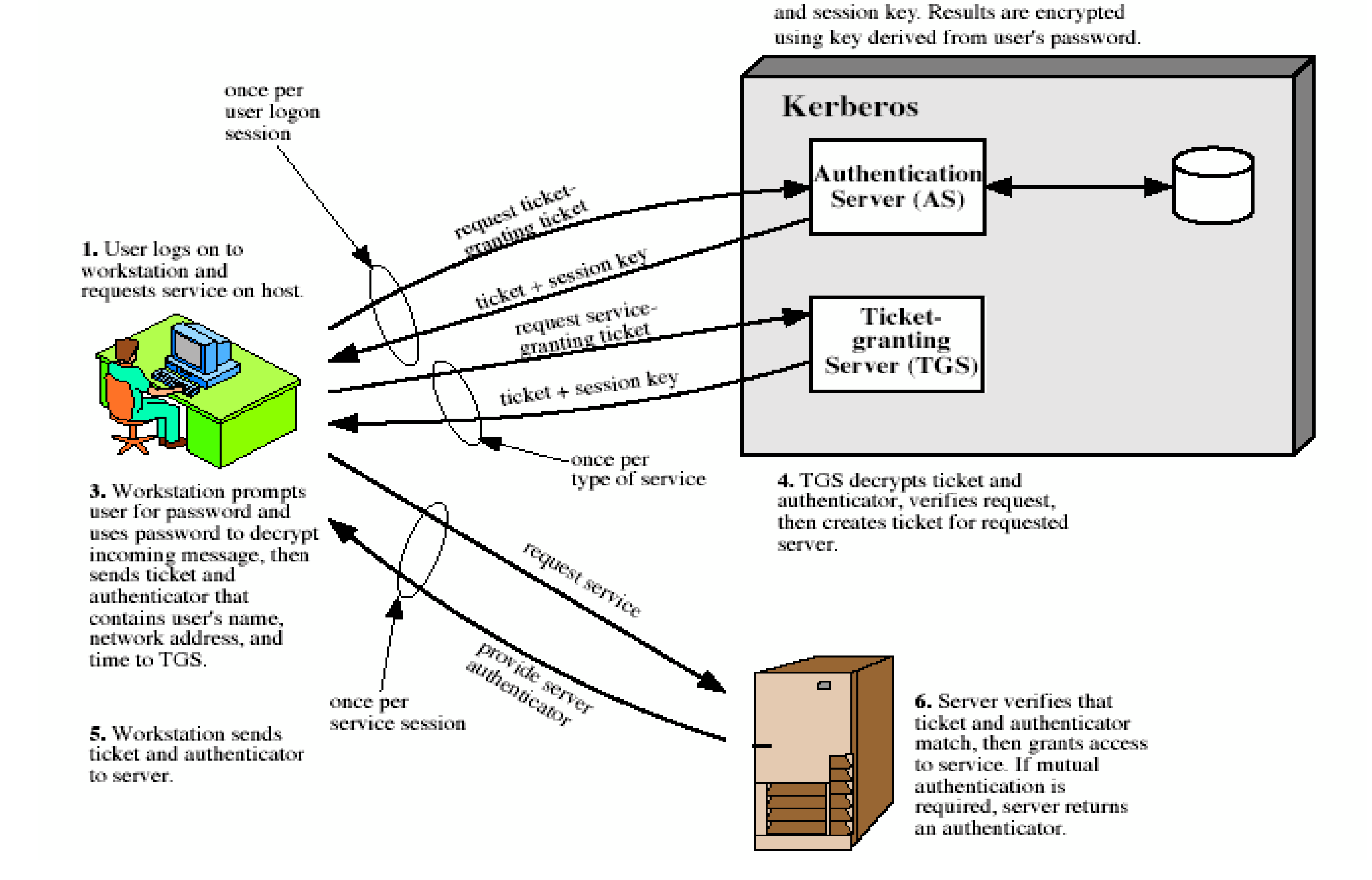
IDv = identifier of user on V

Pc = password of C

ADc = Netowork address of C

Kv = security key shard by As & V

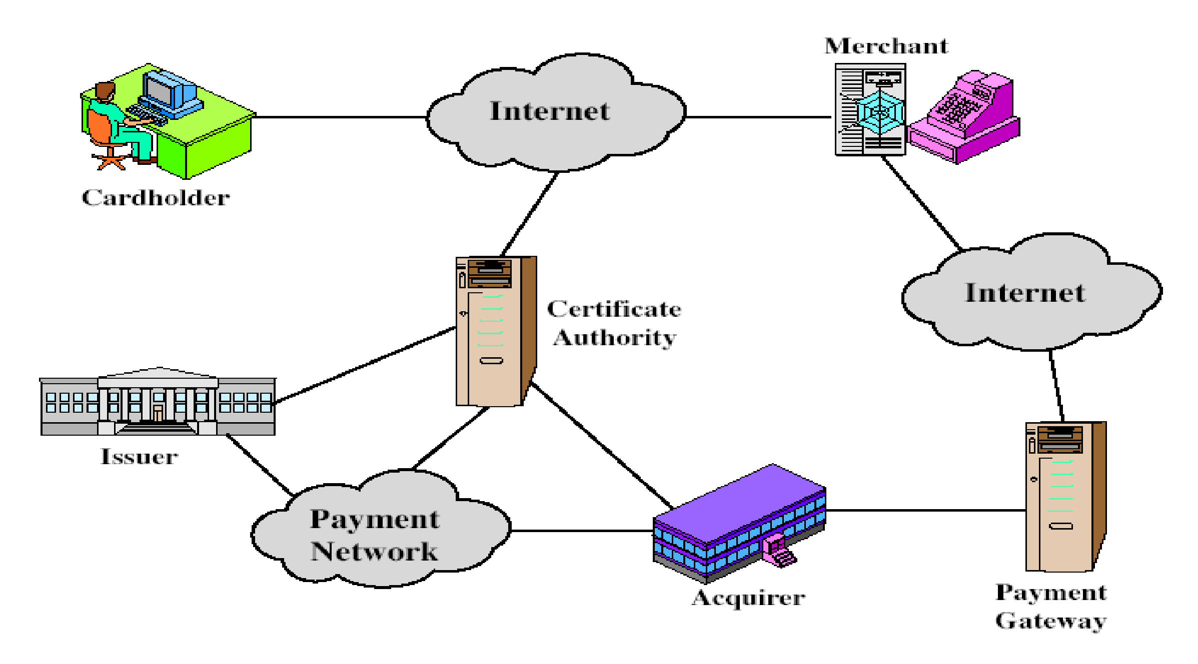
|| concatenation…


2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Kerberos
Authentication Server (AS)
Ticket-granting Server (TGS)
once per user logon session
request ticket-granting ticket
ticket + session key
request service-granting ticket
ticket + session key
once per type of service
1. User logs on to workstation and requests service on host.
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
request service
provide server authenticator
once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.

الفصل السابع عشر : امنية الويب Web Security

بروتوكول أمنية المعاملات الالكترونية Secure Electronic Transactions (SET) :

مواصفات مفتوحة للأمنية والتشفير.
تستخدم لحماية معاملات الـ (credit card) عبر الانترنت.
طورت عام ١٩٩٦م، بواسطة شركتي ستركارد و فيزا الكترون.
لا يعتبر نظام دفع الكتروني، وان كان يساعد في عمليات الدفع الالكتروني.
يعتبر بالاحرى مجموعة من بروتوكولات وتنسيقات الامنية :
حيث يدعم امنية الاتصال بين الشركاء.
موثوق من استخدامه للمعايير كشهادة x.509v3 .
يحمي الخصوصية بحضر المعلومات فقط للطرف الذي يحتاجها.



SET Components

معاملات الـ SET :

١. يقوم الزبون بفتح حساب له في الجهة التي تصدر الـ credit card.
٢. يستلم الزبون وفق ذلك شهادة certificate.
٣. يقوم التجار كل واحد على حده باستلام الشهادات الخاصة بهم.
٤. يقدم الزبون ـ عندما يحتاج ذلك ـ طلب الشراء.
٥. يقوم الوسيط (certificate server) بفحص التاجر أولا.
٦. ترسل طلب الشراء وطلب الدفع بعد ذلك.
٧. يقوم التاجر بطلب التحقق من صحة الدفع.
٨. يقوم التاجر ايظا بالتأكيد على الطلبية.
٩. يقوم التاجر بتقديم الخدمة او البضاعة إلى الزبون.
١٠. يقوم التاجر أخيرا بطلب المبلغ المدفوع له.

التوقيع الثنائي dual signature :

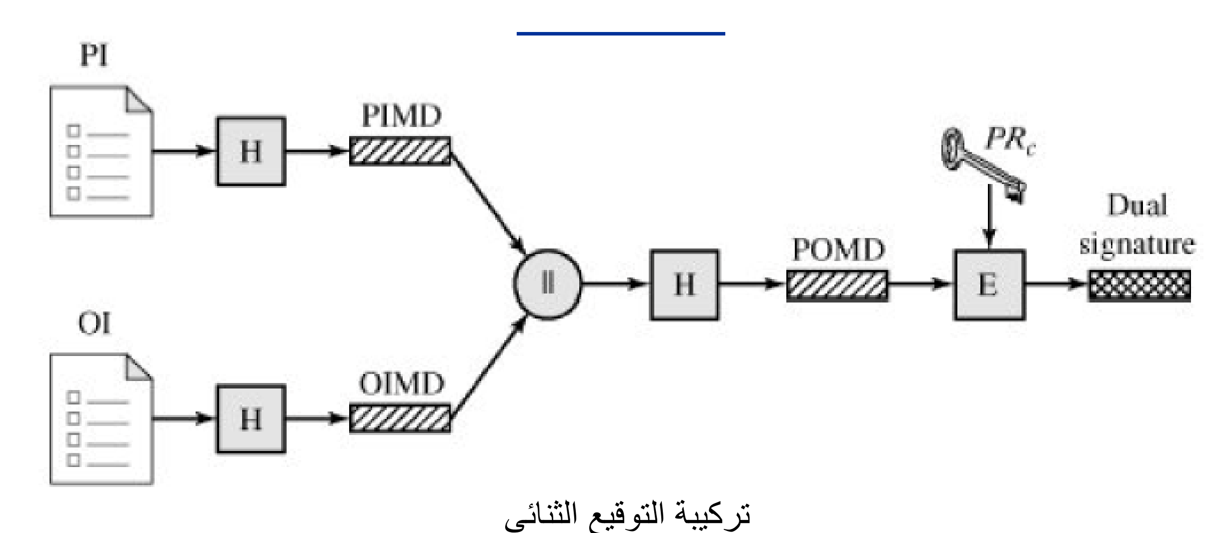
ينشئ الزبون رسالة ثنائية، الاولى فيها معلومات طلب البضاعة OI موجهة للتاجر، والثانية فيها معلومات الدفع PI موجهة للبنك.
لا يقوم اي من التاجر او البنك بفحص معلومات الآخر.
لكن يجب ان يعرفا ان الرسالتين مرتبطتين.

يستخدم لانجاز ذلك التوقيع الثنائي، يقوم هذا التوقيع بدمج الـ **PI** مع الـ **OI** وذلك عبر دالة الهاش المذكورة سابقا.

يكون شكل التوقيع الثنائي رياضيا:

$$DS = E_{kr}[\ H(PI)\ ||\ H(OI)\ ] \rightarrow POMD$$

حيث ان **PIMD** هو **Payment Order Message Digest** وهو ناتج دمج خلاصة معلومات الطلب ومعلومات الدفع وبتشفيره بالمفتاح الخاص للزبون ينتج التوقيع الثنائي.



تركيبة التوقيع الثنائي

ملاحظة هامة:

تمت الترجمة بصورة مستعجلة لذلك يرجى عذر المترجم، والدعاء له بظهر الغيب.